BINDING INTERPRETATIONS DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Group Privacy

Version: 1.0

Stand: 18.11.2016

Status: Endfassung

Inhaltsverzeichnis

1. Einleitung I

2. Inhalt der Datenschutz-Grundverordnung (DSGVO) 4

Kapitel I – Allgemeine Bestimmungen 4

Artikel 3 Räumlicher Anwendungsbereich 4

Artikel 4 Begriffsbestimmungen 6

Kapitel II – Grundsätze 8

Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten 8

Artikel 6 Rechtmäßigkeit der Verarbeitung 11

Artikel 7 Bedingungen für die Einwilligung 14

Artikel 8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft 17

Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten 19

Artikel 10 Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten 21

Artikel 11 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist 22

Kapitel III – Rechte der betroffenen Person 24

Artikel 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person 24

Artikel 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person 26

Artikel 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden 26

Artikel 15 Auskunftsrecht der betroffenen Person 29

Artikel 16 Recht auf Berichtigung 31

Artikel 17 Recht auf Löschung („Recht auf Vergessenwerden“) 33

Artikel 18 Recht auf Einschränkung der Verarbeitung 35

Artikel 20 Recht auf Datenübertragbarkeit 37

Artikel 21 Widerspruchsrecht 39

Artikel 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling 42

Kapitel IV – Verantwortlicher und Auftragsverarbeiter 45

Artikel 24 Verantwortung des für die Verarbeitung Verantwortlichen 45

Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen 48

Artikel 26 Gemeinsam für die Verarbeitung Verantwortliche 50

Artikel 28 Auftragsverarbeiter 52

Artikel 29 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters 52

Artikel 30 Verzeichnis von Verarbeitungstätigkeiten 56

Artikel 32 Sicherheit der Verarbeitung 58

Artikel 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde 60

Artikel 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person 60

Artikel 35 Datenschutz-Folgenabschätzung 64

Artikel 36 Vorherige Konsultation 64

Artikel 37 Benennung eines Datenschutzbeauftragten 67

Artikel 38 Stellung des Datenschutzbeauftragten 69

Artikel 39 Aufgaben des Datenschutzbeauftragten 71

Artikel 42 Zertifizierung 73

Artikel 43 Zertifizierungsstellen 73

Kapitel V – Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen 74

Artikel 44 Allgemeine Grundsätze der Datenübermittlung 74

Artikel 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses 74

Artikel 46 Datenübermittlung vorbehaltlich geeigneter Garantien 74

Artikel 48 Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung 74

Artikel 49 Ausnahmen für bestimmte Fälle 74

Artikel 47 Verbindliche interne Datenschutzvorschriften 78

Kapitel VIII – Rechtsbehelfe, Haftung und Sanktionen 81

Artikel 82 Haftung und Recht auf Schadenersatz 81

Artikel 83 Allgemeine Bedingungen für die Verhängung von Geldbußen 84

Kapitel IX – Vorschriften für besondere Verarbeitungssituationen 86

Artikel 88 Datenverarbeitung im Beschäftigungskontext 86

Kapitel XI – Schlussbestimmungen 88

Artikel 94 Aufhebung der Richtlinie 95/46/EG 88

Artikel 99 Inkrafttreten und Anwendung 88
Artikel 95 Verhältnis zur Richtlinie 2002/58/EG 90
3. Anlagen XCII
Begriffsbestimmungen XCII
Abkürzungen XCVIII
4. Anhang XCVIII

HAFTUNGSAUSSCHLUSS

Der Inhalt der vorliegenden Binding Interpretations beruht auf der endgültigen Fassung der DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) vom April 2016. Er wurde mit größtmöglicher Sorgfalt erstellt. Bis dato wurden noch keine offiziellen Interpretationen zu bestimmten Punkten (z.B. von Aufsichtsbehörden) herausgegeben.

Die Binding Interpretations können eine Einzefallprüfung der Anwendbarkeit der DSGVO auf die Datenverarbeitungen innerhalb Ihres Bereichs bzw. Ihrer Abteilung nicht ersetzen.

Deutsche Telekom AG

Konzernzentrale

Group Privacy

Kontakt: GDPR@telekom.de

<table>
<tr><td colspan="3">Herausgeber
Deutsche Telekom AG, Group Privacy</td></tr>
<tr><td>Dateiname
GDPR Binding Interpretations_DE</td><td>Dokumentennummer
1</td><td>Dokumentname
Binding Interpretations zur DSGVO</td></tr>
<tr><td>Version
1.0</td><td>Letzte Überprüfung
18.11.2016</td><td>Status
Endfassung</td></tr>
<tr><td colspan="3">Kurzbeschreibung
Binding Interpretations zur EU-Datenschutz-Grundverordnung</td></tr>
</table>

Stand: November 2016

1. EINLEITUNG

BINDING INTERPRETATIONS ZUR

DATENSCHUTZ-GRUNDVERORDNUNG

Verordnung (EU) 2016/679

HERAUSGEGEBEN VON GROUP PRIVACY (Konzerndatenschutz)

PRÄAMBEL

Unsere Gesellschaft erfährt eine rasante Digitalisierung. Millionen von Maschinen werden miteinander vernetzt, Unmengen von Daten werden verarbeitet. Diese Entwicklungen werfen Fragen auf, wie es um die in Europa traditionell höheren Datenschutzstandards, verglichen mit der restlichen Welt, bestellt ist. Doch wie lassen sich diese Standards in das digitale Zeitalter überführen? Genügt es, die Gesetze zu befolgen, oder brauchen wir weitergehende Regelungen, um das Vertrauen der Menschen zu gewinnen? Im Kern geht es bei all diesen Fragen und Problemen um das Thema digitale Verantwortung. Eine Verantwortung, die auch die Deutsche Telekom übernimmt, insbesondere im Bereich Datenschutz.

Die Deutsche Telekom ist dafür verantwortlich, das Vertrauen der Menschen in die Datenverarbeitung systematisch zu stärken. Nur so können digitale Geschäfts- und Datenverarbeitungsmodelle zum Wohle der Gesellschaft und jedes Einzelnen erfolgreich weiterentwickelt werden.

Die digitale Souveränität jedes Einzelnen steht dabei im Mittelpunkt. Diese Souveränität wird durch ein hohes Maß an Transparenz, Entscheidungsfreiheit sowie durch die Entwicklung von datenschutzfreundlichen Lösungen gewährleistet. Daher müssen Datenschutzexperten bei der Entwicklung neuer Produkte und Dienste, bei denen personenbezogene Daten verarbeitet werden, von Beginn an einbezogen werden.

Unser Ziel ist es, den Datenschutz im gesamten Konzern Deutsche Telekom zu gewährleisten. Die neue DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) stellt in dieser Hinsicht eine einheitliche Rechtsgrundlage für sämtliche Mitgliedstaaten der EU dar und gilt für alle Einrichtungen, die (gegen Entgelt oder unentgeltlich) Waren oder Dienstleistungen anbieten oder mit der Beobachtung des Verhaltens der Bürgerinnen und Bürger in der EU befasst sind. Organisationen und Wirtschaftsunternehmen weltweit sind

damit unmittelbar für die Einhaltung der DSGVO verantwortlich, wenn sie personenbezogene Daten von Bürgerinnen und Bürgern der EU verarbeiten.

Dies bedeutet auch, dass im Falle eines Verstoßes eines einzelnen Konzernunternehmens gegen die DSGVO die Grundlage für ein Bußgeld der weltweite Jahresumsatz des Telekom Konzerns ist.

DIE BINDING INTERPRETATIONS UND DEREN VERWENDUNG

Der Konzerndatenschutzbeauftragte der DEUTSCHEN TELEKOM legt mit diesen BINDING INTERPRETATIONS (BI) einheitliche Regelungen für die Umsetzung der DSGVO vor. Darin werden nach derzeitigem Wissensstand die rechtlichen Bestimmungen interpretiert, Empfehlungen gegeben und Best Practices aufgezeigt. Außerdem enthält das Dokument Compliance-Fragen, anhand derer die Einhaltung der Vorschriften geprüft werden kann.

Eine konsequente Anwendung der vorgestellten Lösungen (z.B. Interpretationen, Best Practices und Empfehlungen) erleichtert die Umsetzung der DSGVO.

Die Binding Interpretations vereinen Anforderungen und Interpretationen im Hinblick auf eine erfolgreiche EU-weite Umsetzung der DSGVO. Sie sind in Bezug auf die Verarbeitung personenbezogener Daten für alle Konzerunternehmen der DEUTSCHEN TELEKOM innerhalb der Europäischen Union verbindlich. In diesem Zusammenhang sind sie auch insofern auf internationaler Ebene relevant, als EU-Daten von Konzernunternehmen der DEUTSCHEN TELEKOM verarbeitet werden.

Aufgrund des Übergangszeitraums bis zur Anwendbarkeit der DSGVO am 25. Mai 2018 und in Erwartung weiterer, noch nicht festgelegter Rahmenbedingungen wie den von der Artikel-29-Datenschutzgruppe angekündigten Leitlinien spiegeln die vorliegenden Binding Interpretations den aktuellen Auslegungsstand wider. Sie werden entsprechend den weiteren offiziellen Erklärungen und Interpretationen fortgeschrieben. Es handelt sich daher um ein "lebendes" Dokument. Aktualisierte Versionen dieses Dokuments werden per myDMS und über das TELEKOM SOCIAL NETWORK/YOU AND ME zur Verfügung gestellt.

AUFBAU DES DOKUMENTS

Die Binding Interpretations stellen eine Sammlung von rechtlichen Hinweisen und Erläuterungen, Empfehlungen und Umsetzungsvorschlägen für maßgebliche Artikel der DSGVO dar. Das Dokument enthält die wichtigen Artikel der DSGVO jeweils mit einer allgemeinen Beschreibung, einer kurzen Zusammenfassung, den eigentlichen Binding Interpretations, einem vorläufigen Fragebogen zur Compliance, Informationen zu Sanktionen, Best Practices und Vorlagen.

- Im Abschnitt ALLGEMEINE BESCHREIBUNG wird der entsprechende Artikel kurz vorgestellt. Zudem werden Querverweise und Erwägungsgründe aufgeführt. Dieser Aufbau soll Ihnen einen Überblick über alle Artikel geben.
- Anhand der kurzen ZUSAMMENFASSUNG erhalten Sie einen Überblick über den Inhalt des entsprechenden Artikels der DSGVO. Bei Fragen ziehen Sie den jeweiligen vollständigen Artikel der DSGVO heran.
- In den BINDING INTERPRETATIONS (BI) wird der rechtliche Gehalt der DSGVO kurz ausgelegt. Diese Interpretationen sind zur erfolgreichen und rechtskonformen Umsetzung der entsprechenden Bestimmungen der DSGVO von wesentlicher Bedeutung.
- Der COMPLIANCE-FRAGEBOGEN (CFB) enthält vorläufige Fragen, mit deren Hilfe die Einhaltung der Umsetzungsbestimmungen geprüft werden kann. Es wird ein umfassendes Compliance-Genehmigungskonzept erarbeitet und über das TELEKOM SOCIAL NETWORK/YOU AND ME kommuniziert.
- Im SANKTIONSTEIL werden die möglichen Sanktionen aufgezeigt, die bei Nichteinhaltung des entsprechenden Artikels der DSGVO verhängt werden können.
- Schließlich finden Sie in den Abschnitten BEST PRACTICES und VORLAGEN hilfreiche Hinweise bzw. Vorlagen, die zur EU-weiten Verwendung bestimmt sind.

ANSPRECHPARTNER UND FRAGEN

Bei Fragen z.B. zur Auslegung, zur Umsetzung, zum Verhältnis zu anderen Rechtsvorschriften oder bei Abweichungen von den Binding Interpretations wenden Sie sich bitte an das DSGVO-Team (gdpr@telekom.de), Ihren Ansprechpartner bei Group Privacy oder an Ihren Datenschutzbeuaftragten (DSB) vor Ort. Auch eigene Ideen und Best Practices können Sie diesen Ansprechpartnern mitteilen. Informationen über die DSGVO werden per myDMS und über das TELEKOM SOCIAL NETWORK/YOU AND ME zur Verfügung gestellt.

2. INHALT DER DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

KAPITEL I – ALLGEMEINE BESTIMMUNGEN

Artikel 1 bis 4

Das Ziel der Verordnung besteht darin, die richtige Balance zwischen dem Schutz personenbezogener Daten und dem freien Verkehr solcher Daten zu gewährleisten. In diesem Kapitel wird festgelegt, auf welche Arten der Datenverarbeitung die DSGVO Anwendung findet und welche Tätigkeiten im Rahmen der Datenverarbeitung außerhalb des Anwendungsbereichs der DSGVO liegen.

Ferner regelt dieses Kapitel den räumlichen Anwendungsbereich der DSGVO. Es enthält außerdem die wichtigsten Definitionen für die in der Verordnung verwendeten Begriffe.

ARTIKEL 3 RÄUMLICHER ANWENDUNGSBEREICH

I.3.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 3 – Räumlicher Anwendungsbereich (Kapitel I – Allgemeine Bestimmungen)
DSGVO ErwGr	22-25
Querverweise	Artikel 2; Artikel 40 Absatz 3; Artikel 42 Absatz 2; Artikel 45 Absatz 3
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 203 zur Zweckbindung und Weiterverarbeitung
BCRP Verweise	Keine

I.3.2 Zusammenfassung

In diesem Artikel wird der räumliche Anwendungsbereich der DSGVO festgelegt. Die Verordnung gilt für Verantwortliche und Auftragsverarbeiter, die in der Europäischen Union (EU) niedergelassen sind, und unter bestimmten Umständen auch für solche, die außerhalb der EU niedergelassen sind.

I.3.3 Binding Interpretations

IN DER EU NIEDERGELASSENE UNTERNEHMEN:

- **Definition von Niederlassung**: Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus (ErwGr 22).
  → Dies umfasst auch eine nur geringfügige Tätigkeit (EuGH, C-230/14; z.B. einzelner Vertreter).
  → Die Rechtsform ist nicht ausschlaggebend.
- **Datenverarbeitung innerhalb der EU, die Auswirkung auf betroffene Personen außerhalb der EU hat:** Die DSGVO findet auf Unternehmen Anwendung, die in der EU niedergelassen sind und personenbezogene Daten von betroffenen Personen verarbeiten, die ihren Wohnsitz außerhalb der EU haben.

AUSSERHALB DER EU NIEDERGELASSENE UNTERNEHMEN:

- Die DSGVO ist zwingend zu beachten, wenn Unternehmen betroffenen Personen in der EU entgeltliche oder unentgeltliche Waren oder Dienstleistungen anbieten oder das Verhalten betroffener Personen beobachten.

I.3.4 Fragebogen zur Compliance

- Werden bei der Verarbeitung personenbezogener Daten innerhalb der EU von betroffenen Personen mit Wohnsitz außerhalb der EU die Anforderungen der DSGVO erfüllt? [Ja]/[Nein]
- Halten Unternehmen, die betroffenen Personen in der EU Dienstleistungen anbieten oder deren Verhalten beobachten, die DSGVO ein? [Ja]/[Nein]

I.3.5 Sanktionen

Keine

I.3.6 Best Practices und Vorlagen

Keine

ARTIKEL 4 BEGRIFFSBESTIMMUNGEN

I.4.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 4 – Begriffsbestimmungen (Kapitel I – Allgemeine Bestimmungen)
DSGVO ErwGr	26-37
Querverweise	In diesem Artikel werden die in den Artikeln der DSGVO verwendeten Begriffe definiert.
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 203 zur Zweckbindung und Weiterverarbeitung
BCRP Verweise	§ 8 Grundsatz § 9 Zulässigkeit der Verwendung personenbezogener Daten § 10 Einwilligung des Betroffenen § 11 Automatisierte Einzelentscheidungen § 13 Besondere Arten personenbezogener Daten § 15 Koppelungsverbot § 18 Datenverarbeitung im Auftrag § 20 Datensicherheit – Technische und organisatorische Maßnahmen § 27 Verantwortung für die Datenverarbeitung Teil 7 Definitionen und Begriffe

I.4.2 Zusammenfassung

Die wesentlichen Begriffe wie „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“ und „Einwilligung“, die im gesamten Text der DSGVO Verwendung finden, werden in diesem Artikel definiert.

I.4.3 Binding Interpretations

EINWILLIGUNG:

- Die Einwilligung einer betroffenen Person muss schriftlich (z.B. E-Mail) oder durch eine eindeutige bestätigende Handlung (Opt-in) erfolgen.

EINSCHRÄNKUNG DER VERARBEITUNG:

- Die Einschränkung der Verarbeitung bezeichnet die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Die Einschränkung der Verarbeitung bietet mehr Möglichkeiten als die Sperrung von Daten, da sie nicht zwangsläufig die vollständige Sperrung der Datenverarbeitung erfordert.

WEITERE BEGRIFFSBESTIMMUNGEN:

- Weitere Begriffe werden im Zusammenhang mit den in diesem Dokument behandelten Artikeln an der Stelle definiert und erläutert, an der sie relevant sind.

I.4.4 Fragebogen zur Compliance

Keine

I.4.5 Sanktionen

Keine

I.4.6 Best Practices und Vorlagen

Keine

KAPITEL II – GRUNDSÄTZE

Artikel 5 bis 11

In diesem Kapitel werden die Grundsätze für die Datenverarbeitung als Hauptpflichten von Organisationen festgelegt. Die Verarbeitung ist erst dann rechtmäßig, wenn bestimmte, in diesem Kapitel aufgeführte Bedingungen erfüllt sind. Es gibt Bedingungen für die Einwilligung als Rechtsgrundlage der Verarbeitung einschließlich besonderer Bedingungen, die für die Einwilligung eines Kindes gelten.

Darüber hinaus werden Bedingungen für die Verarbeitung besonderer Kategorien personenbezogener Daten wie beispielsweise rassische Herkunft, politische Meinungen und biometrische Daten festgelegt. Besondere Regelungen gelten für die Verarbeitung von personenbezogenen Daten bezüglich strafrechtlicher Verurteilungen und Straftaten sowie für die Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist.

ARTIKEL 5 GRUNDSÄTZE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

II.5.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 5 – Grundsätze für die Verarbeitung personenbezogener Daten (Kapitel II – Grundsätze)
DSGVO ErwGr	39
Querverweise	Artikel 23 Absatz 1; Artikel 25; Artikel 47 Absatz 2 Buchstabe d; Artikel 89 Absatz 1
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 203, „Stellungnahme 03/2013 zur Zweckbindung und Weiterverarbeitung“
BCRP Verweise	§ 14 Datensparsamkeit, Datenvermeidung, Anonymisierung und Pseudonymisierung § 19 Datenqualität § 22 Widerspruchsrecht und Recht auf Löschung, Sperrung und Berichtigung

II.5.2 Zusammenfassung

Der Artikel enthält die Grundsätze der „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, „Zweckbindung“, „Datenminimierung“, „Richtigkeit“, „Speicherbegrenzung“, „Integrität und Vertraulichkeit“ sowie „Rechenschaftspflicht“.

II.5.3 Binding Interpretations

RECHENSCHAFTSPFLICHT:

- Nach dem Grundsatz der Rechenschaftspflicht müssen die Grundsätze der DSGVO nachweisbar eingehalten werden.
- Falls in bestimmten Artikeln der DSGVO geregelt ist, in welcher Form dieser Nachweis erbracht werden soll, ist das Unternehmen dafür verantwortlich, etwaige fehlende Prozesse einzuführen und damit die erforderliche Dokumentation in der Organisation/dem Wirtschaftsunternehmen sicherzustellen.

ANFORDERUNGEN AN DIE DOKUMENTATION NACH DEM GRUNDSATZ DER RECHENSCHAFTSPFLICHT:

Obligatorisch:

- In Schrift- oder elektronischer Form
- Jederzeit auffindbar
- Ergebnis eines klaren Dokumentationsprozesses einschließlich eindeutiger Zuweisung von Verantwortlichkeiten für die Dokumentation
- Klare Beschreibung der aktuellen Situation und der Umstände
- Verweis auf die Rechtsgrundlage
- Angabe des Verfassers und der Änderungshistorie

SPEZIFISCHE DOKUMENTATION DES KONZERNS DEUTSCHE TELEKOM, DIE DIE ANFORDERUNGEN DER RECHENSCHAFTSPFLICHT ERFÜLLEN:

Beispiel:

- Privacy & Security Assessment (PSA)
- Standardisiertes Datenschutz- und Sicherheitskonzept (SDSK)
- Vertrag über die Auftragsverarbeitung (AV)
- Kollektivvereinbarungen
- Verzeichnis der Verarbeitungstätigkeiten (z.B. CAPE[1] für den Verantwortlichen)

II.5.4 Fragebogen zur Compliance

- Siehe konkrete Artikel

[1] Die Software CAPE ist Teil der Zertifizierung des Privacy-Compliance-Management-Systems des Konzerns Deutsche Telekom nach dem Wirtschaftsprüfungsstandard 980.

II.5.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe a: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes

II.5.6 Best Practices und Vorlagen

- https://drc.telekom.de/de/sec/privacy-security-assessment
- https://drc.telekom.de/de/privacy/privacy

ARTIKEL 6 RECHTMÄßIGKEIT DER VERARBEITUNG

II.6.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 6 Rechtmäßigkeit der Verarbeitung (Kapitel II – Grundsätze)
DSGVO ErwGr	32, 40 bis 50, 55, 56
Querverweise	Artikel 8; Artikel 10; Artikel 13 Absatz 1 Buchstabe d, Absatz 2 Buchstabe c; Artikel 14 Absatz 2 Buchstabe d; Artikel 17 Absatz 1 Buchstabe b; Artikel 20 Absatz 1 Buchstabe a; Artikel 21 Absatz 1; Artikel 55 Absatz 2
Zugehörige Unterlagen	Arbeitspapier 203 – Stellungnahme 03/2013 zur Zweckbindung Arbeitspapier 216 zu Anonymisierungsmethoden Arbeitspapier 217 – Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des Verantwortlichen nach Artikel 7 der Richtlinie 95/46/EG
BCRP Verweise	§ 8 Grundsatz § 9 Zulässigkeit der Verwendung personenbezogener Daten § 10 Einwilligung des Betroffenen § 28 Datenschutzbeauftragter

II.6.2 Zusammenfassung

Dieser Artikel regelt die allgemeinen Bedingungen für eine rechtmäßige Verarbeitung personenbezogener Daten, zum Beispiel die Einwilligung, berechtigte Interessen und die Weiterverarbeitung zu einem anderen als dem Zweck, zu dem die personenbezogenen Daten erhoben wurden, wobei der neue Zweck mit dem ursprünglichen Zweck vereinbar sein muss. Gemäß diesem Artikel stellt u.a. die Pseudonymisierung eine geeignete Garantie für die Vereinbarkeit mit dem ursprünglichen Zweck dar.

II.6.3 Binding Interpretations

RECHTSGRUNDLAGEN FÜR DIE VERARBEITUNG VON DATEN, DIE BEI DER ELEKTRONISCHEN KOMMUNIKATION ANFALLEN, UND WEITERE AUSNAHMEN:

- Die Verarbeitung von Daten im Bereich der elektronischen Kommunikation unterliegt der ePrivacy-Richtlinie (ePD) und den zugehörigen nationalen Umsetzungsgesetzen. Das Verhältnis zwischen der ePD und der DSGVO wird in Artikel 95 (Abschnitt XI.95.3) erläutert.

- Die Verarbeitung von Daten im Bereich der elektronischen Kommunikation auf der Grundlage berechtigter Interessen – Artikel 6 Absatz 1 Buchstabe f – oder der Weiterverarbeitung – Artikel 6 Absatz 4 – ist daher nicht rechtmäßig.

- In Bezug auf die besonderen Kategorien personenbezogener Daten haben die Anforderungen von Artikel 9 Vorrang.

- Im Beschäftigungskontext ist Artikel 6 anwendbar, sofern nicht nationales Recht oder andere besondere Bestimmungen (z.B. Artikel 9) Vorrang haben (siehe „Auf einem berechtigten Interesse beruhende Rechtsgrundlagen").

AUF EINEM BERECHTIGTEN INTERESSE BERUHENDE RECHTSGRUNDLAGEN, ARTIKEL 6 ABSATZ 1 BUCHSTABE f:

- Falls Daten zum Zwecke der berechtigten Interessen des Verantwortlichen verarbeitet werden, sind eine Interessenabwägung- und eine Einzelfallprüfung erforderlich. In den folgenden Fällen kann von der widerlegbaren Vermutung ausgegangen werden, dass ein berechtigtes Interesse des Verantwortlichen besteht:

  - **Betrug, Direktwerbung**: z.B. Verarbeitung personenbezogener Daten zur **Verhinderung von Betrug** oder zum Zwecke der **Direktwerbung** (siehe ErwGr 47)
  - **Netz- und Informationssicherheit**: z.B. Verarbeitung zur Verhinderung des Zugangs Unbefugter zu elektronischen Kommunikationsnetzen und der Verbreitung schädlicher Programmcodes sowie Abwehr von Angriffen in Form der gezielten Überlastung von Servern („Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen (siehe ErwGr 49).
  - **Konzerninterne Verabeitung** und **Interessensabwägung**: Konzernunternehmen können ein berechtigtes Interesse haben, personenbezogene Daten von Kunden oder Beschäftigten innerhalb des Konzerns für **Verwaltungszwecke** zu übermitteln (siehe ErwGr 48). Die Anforderungen an die internationale Datenübermittlung bleiben bestehen.
    - → Zu den internen Verwaltungszwecken gehören z.B. die Verarbeitung von Kunden- und Beschäftigtendaten – ErwGr 48 – z.B. zum Zweck der Durchführung einer Innenrevision. Die Verarbeitung von Kunden- und Beschäftigtendaten zu Marketing- und Vertriebszwecken fällt nicht unter die Verwaltungszwecke.
  - Falls für die **Verarbeitung personenbezogener Daten bereits eine gesetzliche Erlaubnis oder eine Einwilligung vorliegt**, kann eine nachfolgende Verarbeitung innerhalb des Konzerns Deutsche Telekom auf Basis einer Interessensabwägung als zulässig angesehen werden; somit ist keine Datenschutzvereinbarung (Auftragsverarbeitung) erforderlich. Jedoch ist ein Dienstleistungsvertrag erforderlich, und die beteiligten Unternehmen sind zur Einhaltung der Konzernrichtlinie Datenschutz – Binding Corporate Rules Privacy (BCRP) verpflichtet. Selbstverständlich ist die betroffene Person zu informieren.

- Transparenz: Die betroffene Person ist unter anderem über das berechtigte Interesse des Verantwortlichen zu informieren, siehe Artikel 13 Absatz 1 Buchstabe d sowie Artikel 14, Absatz 2 Buchstabe b.

LEGITIME GRÜNDE FÜR DIE WEITERVERARBEITUNG ZU EINEM ANDEREN ZWECK, DER MIT DEM URSPRÜNGLICHEN ZWECK VEREINBAR IST, ARTIKEL 6 ABSATZ 4:

- Sofern die Weiterverarbeitung nicht gemäß einer Rechtsvorschrift des betreffenden Mitgliedstaats oder der Einwilligung der betroffenen Person erlaubt ist, müssen bei einer beabsichtigten Weiterverarbeitung zu einem anderen vereinbarten Zweck sämtliche relevanten Aspekte gegeneinander abgewogen werden. Einige dieser relevanten Kriterien sind in Artikel 6 Absatz 4 aufgeführt. Die Verarbeitung auf der Grundlage eines vereinbarten Zwecks kann rechtmäßig sein, wenn unter anderem:

  → eine enge Verbindung zwischen den ursprünglichen Zwecken und dem Zweck der beabsichtigten Weiterverarbeitung besteht (z.B. eigene Dienstleistung des Verantwortlichen im Zusammenhang mit dem vorherigen Zweck) oder die Weiterverarbeitung im engen Zusammenhang mit dem vorherigen Zweck steht, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen (z.B. Vertragsverzeichnis zu früheren Lieferanten), und

  → geeignete Garantien wie z.B. Verschlüsselung oder Pseudonymisierung vorhanden sind. (Die Pseudonymisierung von Daten ist eine Möglichkeit für die Durchführung der vor der Weiterverarbeitung erforderlichen Vereinbarkeitsprüfung – Artikel 6 Absatz 4 Buchstabe e –, siehe II.6.6.). Bei der Anwendung von Verfahren zur Pseudonymisierung ist der DSB entsprechend § 28 Absatz 7 BCRP frühzeitig zu beteiligen.

Die Weiterverarbeitung ist voraussichtlich nicht rechtmäßig,

  → insbesondere wenn besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden und die beabsichtigte Weiterverarbeitung negative Folgen für die betroffenen Personen nach sich ziehen könnte (z.B. negative Auswirkungen in Finanz- oder Rechtsfragen).

II.6.4 Fragebogen zur Compliance

- Beruhen Tätigkeiten zu Direktwerbungszwecken auf angemessenen Rechtsgrundlagen der DSGVO oder sind gesonderte Regelungen maßgeblich? [Ja]/[Nein]

II.6.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe a: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes

II.6.6 Best Practices und Vorlagen

- BEISPIEL: Datenschutzanforderung Anonymisierung und Pseudonymisierung: https://mydms.telekom.de:443/mydms/Start.do?spx=LTDAT5641363444951669545605 45

ARTIKEL 7 BEDINGUNGEN FÜR DIE EINWILLIGUNG

II.7.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 7 – Bedingungen für die Einwilligung (Kapitel II – Grundsätze)
DSGVO ErwGr	32, 33, 42, 43
Querverweise	Artikel 6 Absatz 4; Artikel 8; Artikel 9 Absatz 2 Buchstabe a, c und d; Artikel 83 Absatz 5 Buchstabe a
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 187, „Stellungnahme 15/2011 zur Definition des Begriffes Einwilligung“
BCRP Verweise	§ 10 Einwilligung des Betroffenen § 15 Koppelungsverbot

II.7.2 Zusammenfassung

In Artikel 7 werden die Anforderungen an eine Einwilligung aufgeführt (besondere Anforderungen an die Einwilligung von Kinder, siehe Artikel 8). Darunter fallen die Nachweisbarkeit der Einwilligung, die Form des Ersuchens um Einwilligung, das Recht, die Einwilligung zu widerrufen, sowie die Voraussetzungen für die Freiwilligkeit der Einwilligung.

II.7.3 Binding Interpretations

FORM DER EINWILLIGUNG:

- Die Einwilligung (Begriffsbestimmung siehe Artikel 4 Absatz 11) kann **mündlich, schriftlich und in elektronischer Form** eingeholt werden. Sie muss in Form einer eindeutigen bestätigenden Handlung (Opt-in) gegeben werden:
  - → Gültig: Anklicken eines Kästchens beim Besuch einer Internetseite, „doppeltes Opt-in-Verfahren“ bei E-Mails
  - → Ungültig: Stillschweigen, bereits angekreuzte Kästchen, Untätigkeit der betroffenen Person, Einwilligung in allgemeinen Geschäftsbedingungen, einfaches Opt-in-Verfahren bei E-Mails
- Ersuchen um Einwilligung: Das Ersuchen hat in einer klar verständlichen, leicht zugänglichen Form (der Kunde ist Maßstab) so zu erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Andernfalls ist die Einwilligung nichtig.

  - → BEISPIEL: Einwilligung in den Erhalt von Werbeinhalten nach der konzernweiten Einwilligungsklausel der Deutschen Telekom, Deutschland, siehe II.7.6
  - → BEISPIEL: One-Pager: „Datenschutz leicht gemacht“, siehe II.7.6
- Einwilligung in Kenntnis der Sachlage: Für eine Einwilligung in Kenntnis der Sachlage muss die betroffene Person mindestens über die Identität des Verantwortlichen und die Zwecke der Verarbeitung unterrichtet werden. Es gelten die besonderen Bedingungen der Artikel 13 und 14.
  - → BEISPIEL: „Einwilligung in Kenntnis der Sachlage“, siehe II.7.6

- Freiwilligkeit: Die Einwilligung muss freiwillig erfolgen.
- Die Einwilligung erfolgt unfreiwillig, wenn:
  - → die betroffene Person keine echte oder freie Wahl hat oder nicht in der Lage ist, die Einwilligung zu verweigern oder zu widerrufen, ohne Nachteile zu erleiden.
  - → die Erfüllung eines Vertrags einschließlich der Erbringung einer Dienstleistung von der Einwilligung abhängig gemacht wird, obwohl die Daten für die Erfüllung bzw. Erbringung nicht erforderlich ist. Das Kopplungsverbot gilt nicht, wenn die Einwilligung z.B. im Zusammenhang mit einem Preisausschreiben zu Werbezwecken gegeben wurde.
  - → ein klares Ungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen besteht und es deshalb unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde (z.B. im Beschäftigungskontext).
  - → zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist.

WIDERRUF DER EINWILLIGUNG:

- Form des Widerrufs: Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein. Es muss „derselbe Kanal“ genutzt werden können (wenn die Einwilligung z.B. auf elektronischem Wege erteilt wurde, muss der Widerruf ebenfalls auf elektronischem Wege erfolgen können) oder eine für die betroffene Person noch einfachere Methode angeboten werden.
  - → Wenn die Einwilligung z.B. durch Anklicken eines Kästchens erteilt wurde, muss für den Widerruf ein Kästchen in demselben Formular und an derselben Stelle abgewählt werden können (z.B. Datenschutz-Cockpit).
  - → Informationspflicht in Bezug auf das Widerrufsrecht: Die betroffene Person muss im Vorfeld der Einwilligungserteilung über das Recht informiert werden, die Einwilligung widerrufen zu können.

NACHWEIS ÜBER DIE ERFOLGTE EINWILLIGUNG:

- Beruht die Verarbeitung personenbezogener Daten auf der Einwilligung der betroffenen Person, muss diese in einem geeigneten Nachweis- und Dokumentationsverfahren dokumentiert werden.

  - → BEISPIEL: Prozess für die Einwilligung in den Erhalt von Werbeinhalten nach der konzernweiten Einwilligungsklausel der Deutschen Telekom, Deutschland (KEK). Die Einwilligung kann **mündlich, schriftlich und in elektronischer Form** eingeholt werden. Mündlich gegebene Einwilligungen können anhand einer Sprachdatei und einer schriftlichen Bestätigung nachgewiesen werden; auf elektronischem Wege erteilte Einwilligungen können mithilfe von technischen Prüfverfahren nachgewiesen werden.

→ Vor Anwendung der DSGVO erteilte Einwilligung: Wenn das Einwilligungsverfahren den Anforderungen der DSGVO entspricht, kann die Einwilligung durch Darstellung des allgemeinen Einwilligungsverfahrens nachgewiesen werden. Die jeweilige auf diesem Verfahren beruhende Einwilligung sollte gekennzeichnet werden. In diesem Zusammenhang sollte die Aufsichtsbehörde kontaktiert werden.

II.7.4 Fragebogen zur Compliance

- Gibt es ein Verfahren zur Dokumentation der Einwilligung der betroffenen Person? [Ja]/[Nein]
- Gibt es ein Verfahren, durch das sichergestellt wird, dass die Anforderungen für die Einholung einer Einwilligung im jeweiligen konkreten Fall tatsächlich berücksichtigt werden? [Ja]/[Nein]
- Gibt es Verfahrensanforderungen für das Widerrufsverfahren? [Ja]/[Nein]

II.7.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe a: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes

II.7.6 Best Practices und Vorlagen

- BEISPIEL: „Nachweis über die erteilte Einwilligung“: aktuelles Verfahren zur Einholung der Einwilligung zu Werbezwecken:



- BEISPIEL: „Einwilligung in Kenntnis der Sachlage“: aktuelles Verfahren der Deutschen Telekom für die Einholung einer Einwilligung in Kenntnis der Sachlage, KEK
- BEISPIEL: One-Pager: „Datenschutz leicht gemacht“: https://www.telekom.de/datenschutz-ganz-einfach

ARTIKEL 8 BEDINGUNGEN FÜR DIE EINWILLIGUNG EINES KINDES IN BEZUG AUF DIENSTE DER INFORMATIONSGESELLSCHAFT

II.8.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 8 – Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft (Kapitel II – Grundsätze)
DSGVO ErwGr	38
Querverweise	Artikel 6 Absatz 1 Buchstabe a; Artikel 12 Absatz 1; Artikel 40 Absatz 2 Buchstabe g
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 187, „Stellungnahme 15/2011 zur Definition des Begriffes Einwilligung“
BCRP Verweise	§ 10 Einwilligung des Betroffenen Kinder: keine Regelung

II.8.2 Zusammenfassung

Eine Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a für die Verarbeitung von Daten im Zusammenhang mit Diensten der Informationsgesellschaft muss durch den Träger der elterlichen Verantwortung oder mit dessen Zustimmung erfolgen, wenn das Kind noch nicht das sechzehnte Lebensjahr vollendet hat. Nach nationalen Rechtsvorschriften kann eine niedrigere Altersgrenze vorgesehen werden, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.

II.8.3 Binding Interpretations

SZENARIEN, IN DENEN DIE BESONDEREN BEDINGUNGEN FÜR DIE EINWILLIGUNG EINES KINDES GREIFEN:

- Die Einwilligung bzw. Zustimmung zur Einwilligung durch den Träger der elterlichen Verantwortung für das Kind ist im Zusammenhang mit Diensten der Informationsgesellschaft (z.B. soziale Netzwerke) insbesondere erforderlich:
  - → für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten bei der Nutzung von Diensten, die Kindern direkt angeboten werden (siehe ErwGr 38) wenn die Einwilligung des Kindes die Rechtsgrundlage für die Verarbeitung seiner personenbezogenen Daten darstellt.

ALLGEMEINES VERTRAGSRECHT:

- Die Anforderungen gemäß dem allgemeinen Vertragsrecht, z.B. hinsichtlich der Gültigkeit, des Abschlusses oder der Wirkung eines Vertrags im Zusammenhang mit einem Kind (z.B. elektronisch per Fernabsatz) gelten fort.

ALTERSÜBERPRÜFUNG:

- Der Verantwortliche hat die durch den Träger der elterlichen Verantwortung oder mit dessen Zustimmung erteilte Einwilligung zu überprüfen.

II.8.4 Fragebogen zur Compliance

- Gibt es in Ihrem Unternehmen geeignete Verfahren, um im Bedarfsfall das Alter von Kunden zu überprüfen? [Ja]/[Nein]
- Wurden geeignete technische Vorkehrungen getroffen, um im Bedarfsfall sicherzustellen, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde, falls das Kind noch nicht das für die Erteilung der Einwilligung festgelegte Mindestalter erreicht hat? [Ja]/[Nein]

II.8.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes

II.8.6 Best Practices und Vorlagen

Keine

ARTIKEL 9 VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

II.9.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 9 – Verarbeitung besonderer Kategorien personenbezogener Daten (Kapitel II – Grundsätze)
DSGVO ErwGr	51–56
Querverweise	Artikel 6 Absatz 4
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 187, „Stellungnahme 15/2011 zur Definition des Begriffes Einwilligung“
BCRP Verweise	§ 13 Besondere Arten personenbezogener Daten

II.9.2 Zusammenfassung

Die Verarbeitung besonderer Kategorien personenbezogener Daten (rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person) ist außer in den ausdrücklich im Artikel aufgeführten Fällen untersagt.

II.9.3 Binding Interpretations

BEDINGUNGEN FÜR DIE VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN:

- **Artikel 9 stellt einen eigenen Bedingungskatalog** für die rechtmäßige Verarbeitung dieser besonderen Kategorien auf. Artikel 6 ist, soweit Artikel 9 Anwendung findet, für die Verarbeitung besonderer Kategorien von Daten nicht maßgeblich:
  - → Beispielsweise kann sich das Unternehmen nicht auf die Wahrnehmung seiner berechtigten Interessen berufen, um sensible personenbezogene Daten zu verarbeiten.

AUSDRÜCKLICHE EINWILLIGUNG:

- **Ausdrückliche Einwilligung**: Neben den allgemeinen Regelungen in Bezug auf die Einwilligung nach ihrer Begriffsbestimmung in Artikel 4 Absatz 11 gilt zusätzlich, dass die jeweilige Kategorie der

besonderen Kategorien von zu verarbeitenden personenbezogenen Daten ausdrücklich angegeben sein muss.

BIOMETRISCHE UND GENETISCHE DATEN:

- **Biometrische und genetische Daten** fallen nunmehr ausdrücklich unter die besonderen Kategorien personenbezogener Daten. Jedes Unternehmen, das dem Konzern Deutsche Telekom angehört und biometrische bzw. genetische Daten verarbeitet hat bzw. verarbeiten wird, hat die Rechtmäßigkeit dieser Verarbeitung im Rahmen des PSA-Verfahrens zu beurteilen.

II.9.4 Fragebogen zur Compliance

- Verarbeitet Ihr Unternehmen besondere Kategorien personenbezogener Daten und erfüllt es bei Vorliegen der Einwilligung zu einer solchen Verarbeitung die Anforderungen der DSGVO? [Ja]/[Nein]
- Wurden technische und organisatorische Maßnahmen (TOM) zum Schutz dieser Daten auf eine bestimmte und sichere Weise getroffen? [Ja]/[Nein]

II.9.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe a: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes

II.9.6 Best Practices und Vorlagen

Keine

ARTIKEL 10 VERARBEITUNG VON PERSONENBEZOGENEN DATEN ÜBER STRAFRECHTLICHE VERURTEILUNGEN UND STRAFTATEN

II.10.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 10 – Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Kapitel II – Grundsätze)
DSGVO ErwGr	Keine
Querverweise	Artikel 6 Absatz 1
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 203 zur Zweckbindung und Weiterverarbeitung
BCRP Verweise	Keine

II.10.2 Zusammenfassung

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist.

II.10.3 Binding Interpretations

FÜHRUNGSZEUGNIS:

- Die Vorlage des Führungszeugnisses eines Bewerbers bzw. Beschäftigten im Rahmen des Recruitingprozesses ist nur dann rechtmäßig, wenn die Verarbeitung nach Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist.

II.10.4 Fragebogen zur Compliance

- Falls die Vorlage eines Führungszeugnisses Teil des Recruitingprozesses in Ihrem Unternehmen ist, ist dies nach Unionsrecht oder dem Recht der Mitgliedstaaten zulässig? [Ja]/[Nein]

II.10.5 Sanktionen

Keine

II.10.6 Best Practices und Vorlagen

Keine

ARTIKEL 11 VERARBEITUNG, FÜR DIE EINE IDENTIFIZIERUNG DER BETROFFENEN PERSON NICHT ERFORDERLICH IST

II.11.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 11 - Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist (Kapitel II – Grundsätze)
DSGVO ErwGr	57
Querverweise	Artikel 12 Absatz 2; 15-20
Zugehörige Unterlagen	Keine
BCRP Verweise	§ 19 Datenqualität

II.11.2 Zusammenfassung

Der Verantwortliche ist nicht verpflichtet, zur bloßen Einhaltung der DSGVO die Daten zur Identifizierung der betroffenen Person aufzubewahren. Falls der Verantwortliche die betroffene Person nicht identifizieren kann, muss er die betroffene Person entsprechend informieren.

II.11.3 Binding Interpretations

- Telekommunikationsanbieter sind dazu aufgefordert eine Person zu identifizieren, mit der ein Telekommunikationsvertrag abgeschlossen wurde. Dementsprechend findet Artikel 11 keine Anwendung im Falle einer nicht durchführbaren Identifikation.
- Der Verantwortliche ist verpflichtet die Person zu identifizieren, **ist jedoch nicht dazu aufgefodert zusätzliche Informationen zu sammeln.** Dies könnte der Fall sein, falls die betroffene Person das Recht hat unterrichtet zu werden, der Verantwortliche jedoch nur pseudonyme Daten im Datenzentrum hat, ohne die Chance die betroffene Persion zu identifizieren (der Schlüssel wurde gelöscht).
- Artikel 11 Absatz 2 beschränkt nur die Rechte des Betroffenen, z.B. im Falle des Auskunftsrechts des Betroffenen, jedoch nicht im Falle der Transparenzpflicht des Verantwortlichen. Daher ist der Verantwortliche auch zur Transparenz verpflichtet, falls personenbezogene Daten pseudonym verarbeitet werden.

II.11.4 Fragebogen zur Compliance

Keine

II.11.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes

II.11.6 Best Practices und Vorlagen

Keine

KAPITEL III – RECHTE DER BETROFFENEN PERSON

Artikel 12 bis 23

Die Verordnung räumt den betroffenen Personen eine Vielzahl von Rechten ein, z.B. Recht auf Informationen und Auskunft zu personenbezogen Daten, Recht auf Berichtigung, Recht auf Vergessenwerden, Recht auf Datenübertragbarkeit und Widerspruchsrecht.

In diesem Kapitel ist festgelegt, wie und wann der Verantwortliche jedem einzelnen dieser Rechte Geltung zu verschaffen hat. In Artikel 22 sind zudem die Rechte und Einschränkungen in Bezug auf Profiling festgehalten.

ARTIKEL 12 TRANSPARENTE INFORMATION, KOMMUNIKATION UND MODALITÄTEN FÜR DIE AUSÜBUNG DER RECHTE DER BETROFFENEN PERSON

III.12.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 12 – Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (Kapitel III – Rechte der betroffenen Person)
DSGVO ErwGr	58, 59
Querverweise	Artikel 11 Absatz 2; 13122; 34; 83
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 187, „Stellungnahme 15/2011 zur Definition des Begriffes Einwilligung“
BCRP Verweise	§ 5 Informationspflicht § 11 Automatisierte Einzelentscheidungen § 12 Die Verwendung personenbezogener Daten für Direktmarketingzwecke § 22 Widerspruchsrecht und Recht auf Löschung, Sperrung und Berichtigung

III.12.2 Zusammenfassung

Artikel 12 enthält ausführliche Anforderungen hinsichtlich der Pflichten des Verantwortlichen, der betroffenen Person transparente Informationen und Mitteilungen zu übermitteln und die Modalitäten für die Ausübung ihrer Rechte transparent zu erläutern.

III.12.3 Binding Interpretations

ALLGEMEINE ANFORDERUNGEN:

- Form: Informationen müssen schriftlich, auf elektronischem Wege oder auf Wunsch mündlich übermittelt werden, wenn die Identität der betroffenen Person nachgewiesen ist.
- Der Verantwortliche wird nicht tätig: Der Verantwortliche unterrichtet die betroffene Person unverzüglich, spätestens aber innerhalb eines Monats über die Gründe dafür, dass er nicht tätig wird. Er unterrichtet sie über die Möglichkeit, sich an die Aufsichtsbehörde zu wenden oder einen gerichtlichen Rechtsbehelf einzulegen.

BESONDERE ANFORDERUNGEN GEMÄSS ARTIKEL 12:

- Diese werden ausführlich in den Artikeln 13 bis 22 und in Artikel 34 erörtert, sofern sie für die Binding Interpretations dieser Artikel von Belang sind.

III.12.4 Fragebogen zur Compliance

- Gibt es einen Prozess, um festzustellen, ob die Anforderungen an transparente Informationen erfüllt werden? [Ja]/[Nein]

III.12.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe b: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes

III.12.6 Best Practices und Vorlagen

- One-Pager: „Datenschutz leicht gemacht“: https://www.telekom.de/datenschutz-ganz-einfach

ARTIKEL 13 INFORMATIONSPFLICHT BEI ERHEBUNG VON PERSONENBEZOGENEN DATEN BEI DER BETROFFENEN PERSON

ARTIKEL 14 INFORMATIONSPFLICHT, WENN DIE PERSONENBEZOGENEN DATEN NICHT BEI DER BETROFFENEN PERSON ERHOBEN WURDEN

III.13, 14.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 13 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Kapitel III – Rechte der betroffenen Person) Artikel 14 – Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Kapitel III – Rechte der betroffenen Person)
DSGVO Artikel	60–62
Querverweise	Artikel 6 Absatz 1 Buchstabe f; Artikel 9 Absatz 2 Buchstabe a; Artikel 12; Artikel 22 Absatz 1 und 4; Artikel 26 Absatz 1; Artikel 46; Artikel 47 Absatz 2 Buchstabe g; Artikel 49 Absatz 1; Artikel 79; Artikel 89 Absatz 1
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 187, „Stellungnahme 15/2011 zur Definition des Begriffes Einwilligung“
BCRP Verweise	§ 5 Informationspflicht § 11 Automatisierte Einzelentscheidungen

III.13,14.2 Zusammenfassung

Diese Artikel regeln, welche Arten von Informationen der betroffenen Person zu übermitteln sind, wenn die Daten unmittelbar von der betroffenen Personen bzw. von einer anderen Quelle erhoben wurden.

III.13,14.3 Binding Interpretations

ZEITPUNKT FÜR DIE MITTEILUNG VON INFORMATIONEN WENN DIE DATEN UNMITTELBAR BEI DER BETROFFENEN PERSON ERHOBEN WERDEN:

- Die Mitteilung hat zu dem Zeitpunkt zu erfolgen, zu dem personenbezogene Daten bei der betroffenen Person erhoben werden.

ZEITPUNKT FÜR DIE MITTEILUNG VON INFORMATIONEN, WENN DIE DATEN NICHT BEI DER BETROFFENEN PERSON ERHOBEN WERDEN:

- Die Mitteilung hat innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats zu erfolgen.
- Falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen: Die Mitteilung hat spätestens zum Zeitpunkt der ersten Mitteilung an sie zu erfolgen.
- Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist: Die Mitteilung hat spätestens zum Zeitpunkt der ersten Offenlegung zu erfolgen.
- Wenn der Verantwortliche beabsichtigt, Daten zu einem anderen/neuen Zweck zu verarbeiten: Der Verantwortliche hat die betroffene Person diesbezüglich vor der Weiterverarbeitung zu informieren.

GESTALTUNG DER AN DIE BETROFFENE PERSON GERICHTETEN INFORMATIONEN:

- Klare Sprache, beliebige Form, kostenlos, unter Verwendung von Bildsymbolen, nachdem die EU-Kommission einen delegierten Rechtsakt zur Verwendung von Bildsymbolen erlassen hat.
- Die Gestaltung der Information hängt vom Zusammenhang ab, in dem Daten von der betroffenen Person erhoben werden, beispielsweise schriftlich in Form einer Datenschutzerklärung auf einer Website (siehe III.13.6 bis 14.6, „One-Pager des Konzerns Deutsche Telekom“), verschickt als E-Mail, mündlich am Telefon, sollte dies von der betroffenen Person gewünscht und deren Identität nachgewiesen sein.
- Bei der Bereitstellung von Informationen zur beabsichtigten Übermittlung personenbezogener Daten an Drittländer müssen die konkreten einzelnen Drittländer nicht angegeben werden.
- Der betroffenen Person müssen die unter Artikel 13 und 14 aufgeführten Informationen zum Zeitpunkt des Anwendbarkeit der DSGVO mitgeteilt werden.

GESTALTUNG DER INFORMATION BEI VERARBEITUNG VON DATEN EINES KINDES:

- Um der besonderen Schutzbedürftigkeit von Kindern Rechnung zu tragen, müssen die an Kinder gerichteten Informationen und Mitteilungen so klar und einfach gehalten sein, dass sie für Kinder leicht verständlich sind.

III.13,14.4 Fragebogen zur Compliance

- Wurde das bisherige Verfahren und der Informationsgehalt der Mitteilungen an die betroffene Person insbesondere hinsichtlich der Form und des Zeitpunkts überprüft? [Ja]/[Nein]
- Wurden bestehende Datenschutz-Policies/Datenschutzerklärungen dahingehend geprüft, ob sie alle nach der DSGVO erforderlichen Informationen enthält? [Ja]/[Nein]

III.13,14.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe b: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes.

III.13,14.6 Best Practices und Vorlagen

- BEISPIEL: „Online-Datenschutzerklärung – One-Pager der Deutschen Telekom“: https://www.telekom.de/datenschutz-ganz-einfach
- BEISPIEL: „Datenschutzerklärung“: aktuelle Datenschutzerklärung der Deutschen Telekom (Telekommunikationsdaten auf Deutsch): http://www.telekom.de/dlp/agb/pdf/43963.pdf

ARTIKEL 15 AUSKUNFTSRECHT DER BETROFFENEN PERSON

III.15.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 15 – Auskunftsrecht der betroffenen Person (Kapitel III – Rechte der betroffenen Person)
DSGVO ErwGr	63, 64
Querverweise	Artikel 11 Absatz 2; Artikel 22 Absatz 1 und 4; Artikel 46; Artikel 89 Absatz 2 und 3
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 187, „Stellungnahme 15/2011 zur Definition des Begriffes Einwilligung“
BCRP Verweise	§ 5 Informationspflicht § 11 Automatisierte Einzelentscheidungen

III.15.2 Zusammenfassung

Dieser Artikel regelt das Recht der betroffenen Person auf Auskunft zu den vom Verantwortlichen verarbeiteten personenbezogenen Daten und legt fest, über was im einzelnen Auskunft gegeben werden muss (z.B. Zweck, Kategorien, Empfänger, Speicherung, für Beschwerden zuständige Behörden, Recht auf Berichtigung oder Löschung, Herkunft der erhobenen Daten, Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling, Informationen über geeignete Garantien bei der Übermittlung an Drittländer).

III.15.3 Binding Interpretations

RECHT AUF AUSKUNFT:

- Informationen: Die betroffene Person hat das Recht auf ausführliche Informationen zu den personenbezogenen Daten, siehe III.15.2. Die Informationen über die Übermittlung personenbezogener Daten an Drittländer müssen keine konkreten Informationen zu den betroffenen Ländern enthalten, wohl aber eine Beschreibung der geeigneten Garantien (z.B. BCRP, Standardvertragsklauseln).
- Form und Kosten: Der Verantwortliche muss Informationen/Kopien unentgeltlich zur Verfügung stellen; bei wiederholten, offenkundig unbegründeten oder exzessiven Anfragen und weiteren Kopien kann er eine angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen. Bei Anfrage auf elektronischem Wege muss die Antwort auf elektronischem Wege gegeben werden, sofern nichts

anderes gewünscht wird. Um der Anfrage zu entsprechen, kann der Verantwortliche der betroffenen Person auch einen Fernzugang zu den personenbezogenen Daten bereitstellen (z.B. über den Link „Personenbezogene Daten“ im Online-Kundenkonto).

- Zeitpunkt: Die Informationen sollten innerhalb eines Monats nach Eingang der Anfrage beim Verantwortlichen bereitgestellt werden (siehe Artikel 13 Absatz 3).
- Bestätigung der Identität: Der Verantwortliche kann zusätzliche Informationen zur Feststellung der Identität der Auskunft suchenden betroffenen Person einholen.

III.15.4 Fragebogen zur Compliance

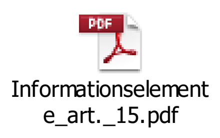
- Gibt es ein Verfahren für die Bearbeitung von Auskunftsersuchen betroffener Personen und entspricht dieses Verfahren der DSGVO? [Ja]/[Nein]

III.15.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe b: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes

III.15.6 Best Practices und Vorlagen

- Überblick Inhalt Artikel 15:



ARTIKEL 16 RECHT AUF BERICHTIGUNG

III.16.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 16 – Recht auf Berichtigung (Kapitel III – Rechte der betroffenen Person)
DSGVO ErwGr	65
Querverweise	Artikel 5 Absatz 1 Buchstabe d; Artikel 12; Artikel 14 Absatz 2 Buchstabe c; Artikel 15 Absatz 1 Buchstabe e; Artikel 58 Absatz 2 Buchstabe g
Zugehörige Unterlagen	Keine
BCRP Verweise	§ 5 Informationspflicht § 22 Widerspruchsrecht und Recht auf Löschung, Sperrung und Berichtigung

III.16.2 Zusammenfassung

Dieser Artikel regelt das Recht der betroffenen Person auf Berichtigung unrichtiger oder unvollständiger personenbezogener Daten.

III.16.3 Binding Interpretations

BESTEHENDE VERFAHREN:

- Es sind keine Änderungen an den bestehenden Verfahren erforderlich, wenn die Prozesse bereits im Einklang mit den nationalen Gesetzen zur Umsetzung der Richtlinie 95/46/EG stehen.
- Die betroffene Person ist berechtigt, unvollständige Daten auch durch eine ergänzende Erklärung zu vervollständigen.

ANTRAG AUF BERICHTIGUNG ABGEWIESEN:

- Sollte dem Antrag der betroffenen Person nicht stattgegeben werden, sind die Gründe für diese Entscheidung zu dokumentieren und der betroffenen Person auf transparente Weise mitzuteilen.

III.16.4 Fragebogen zur Compliance

- Entsprechen die bestehenden Verfahren in Bezug auf das Recht auf Berichtigung Artikel 16? [Ja]/[Nein]

III.16.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe b: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes.

III.16.6 Best Practices und Vorlagen

Keine

ARTIKEL 17 RECHT AUF LÖSCHUNG („RECHT AUF VERGESSENWERDEN“)

III.17.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 17 – Recht auf Löschung („Recht auf Vergessenwerden“) (Kapitel III – Rechte der betroffenen Person)
DSGVO ErwGr	65, 66
Querverweise	Artikel 12; Artikel 13 Absatz 2 Buchstabe b; Artikel 14 Absatz 2 Buchstabe c; Artikel 15 Absatz 1 Buchstabe e; Artikel 18 Absatz 1 Buchstabe b; Artikel 58 Absatz 2 Buchstabe g; Artikel 70 Absatz 1 Buchstabe d;
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 225 „Richtlinien für die Umsetzung des Urteils des Gerichtshof der Europäischen Union zu ‚Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González‘ (c131/12)“
BCRP Verweise	§ 5 Informationspflicht § 22 Widerspruchsrecht und Recht auf Löschung, Sperrung und Berichtigung

III.17.2 Zusammenfassung

Der Verantwortliche hat personenbezogene Daten „unverzüglich“ auf Verlangen der betroffenen Person zu löschen, wenn die Daten nicht mehr notwendig sind, die betroffene Person Widerspruch gegen die Verarbeitung einlegt, die Verarbeitung unrechtmäßig war oder ein anderer in diesem Artikel aufgeführter Grund vorliegt.

III.17.3 Binding Interpretations

VERFAHREN ZUR LÖSCHUNG VON DATEN:

Artikel 17 enthält grundsätzlich keine neuen Anforderungen für die Art und Weise, wie Daten zu löschen sind. Besondere Aspekte:

- Widerspruch gegen die Verarbeitung: Personenbezogene Daten müssen gelöscht werden, wenn die betroffene Person der Verarbeitung in den folgenden Fällen widerspricht (siehe Artikel 17 Absatz 1 Buchstabe c und Artikel 21 Absatz 1 und 2):
  - Die betroffene Person legt gegen die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe e „öffentliches Interesse“ oder Artikel 6 Absatz 1 Buchstabe f „berechtigtes Interesse“ einschließlich Profiling Widerspruch ein und es liegen keine vorrangigen berechtigten Gründe für die Weiterverarbeitung vor, oder
  - die betroffene Person legt Widerspruch gegen die Verarbeitung zu Direktwerbezwecken ein. Dies umfasst auch Profiling, soweit es mit diesen Zwecken im Zusammenhang steht.
- Widerruf der Einwilligung: Entsprechende Daten müssen gelöscht werden, wenn die betroffene Person ihre Einwilligung widerruft, die auf Artikel 6 Absatz 1 Buchstabe a „Einwilligung“ oder Artikel 9 Absatz 2 „Einwilligung für besondere Kategorien von Daten“ beruhte, und keine sonstigen berechtigten Gründe für die Verarbeitung vorliegen (Artikel 17 Absatz 1 Buchstabe b).
- Kopien oder Replikationen: Beim Löschen müssen auch die Kopien und Replikationen gelöscht werden.
- Sperrung: Die Sperrung von Daten ist auf der Grundlage der in Artikel 17 Absatz 3 aufgeführten Zwecke zulässig.
- Datenverarbeitungsprogramme, die keine Löschfunktion haben, dürfen nicht eingeführt werden, wenn die Löschung von der DSGVO verlangt wird.

SUCHMASCHINEN:

- Die in Artikel 17 Absatz 2 festgelegten Pflichten richten sich hauptsächlich an die Betreiber von Suchmaschinen, z.B. Google, Bing und Yahoo. Die vom Gerichtshof der Europäischen Union im sogenannten „Google-Urteil“ (C-131/12) festgelegten Standards bleiben gültig.

III.17.4 Fragebogen zur Compliance

- Stehen die Verfahren in Ihrem Unternehmen im Einklang mit Artikel 17 DSGVO? [Ja]/[Nein]

III.17.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe b: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes.

III.17.6 Best Practices und Vorlagen

Keine

ARTIKEL 18 RECHT AUF EINSCHRÄNKUNG DER VERARBEITUNG

III.18.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 18 – Recht auf Einschränkung der Verarbeitung (Kapitel III – Rechte der betroffenen Person)
DSGVO ErwGr	67
Querverweise	Artikel 4 Absatz 3; Artikel 12; Artikel 19; Artikel 21 Absatz 1; Artikel 58 Absatz 2 Buchstabe g;
Zugehörige Unterlagen	Keine
BCRP Verweise	§ 5 Informationspflicht

III.18.2 Zusammenfassung

Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen.

III.18.3 Binding Interpretations

EINSCHRÄNKUNG DER WEITERVERARBEITUNG:

- Das Recht auf Einschränkung ist ein für betroffene Personen neu eingeführtes Recht. Es unterscheidet sich vom früheren Recht auf Sperrung von Daten insoweit, als damit die Verarbeitung zu den Zwecken nach Artikel 18 Absatz 2 nach wie vor möglich ist. Falls die Verarbeitung von Daten eingeschränkt werden muss, ist es dem Verantwortlichen nur gestattet, die Daten zu speichern und in den festgelegten Fällen zu nutzen.
  → Beispielsweise nur mit Einwilligung der betroffenen Person zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Das Recht, die Einschränkung der Verarbeitung zu verlangen, steht ausschließlich der betroffenen Person zu.

TECHNISCHE REALISIERBARKEIT DER EINSCHRÄNKUNG DER VERARBEITUNG:

- Das Unternehmen hat Prozesse einschließlich technischer und organisatorischer Maßnahmen umzusetzen, um das Recht der betroffenen Person, die Verarbeitung ihrer Daten einzuschränken, zu realisieren.

III.18.4 Fragebogen zur Compliance

- Entsprechen die bestehenden Verfahren in Bezug auf das Recht auf Einschränkung der Verarbeitung Artikel 18? [Ja]/[Nein]
- Wurde die Möglichkeit der Einschränkung der Datenverarbeitung technisch umgesetzt? [Ja]/[Nein]
- Wurde ein Verfahren eingeführt, das die Information der betroffenen Person vor Aufhebung der Einschränkung sicherstellt? [Ja]/[Nein]

.III.18.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe b: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes.

III.18.6 Best Practices und Vorlagen

Keine

ARTIKEL 20 RECHT AUF DATENÜBERTRAGBARKEIT

III.20.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 20 – Recht auf Datenübertragbarkeit (Kapitel III – Rechte der betroffenen Person)
DSGVO ErwGr	68
Querverweise	Artikel 6 Absatz 1 Buchstabe a und b; Artikel 14 Absatz 2 Buchstabe c; Artikel 17
Zugehörige Unterlagen	Arbeitspapier 236
BCRP Verweise	§ 5 Informationspflicht

III.20.2 Zusammenfassung

Auf Antrag übermittelt der Verantwortliche die Daten, die die betroffene Person ihm bereitgestellt hat, in einem gängigen und maschinenlesbaren Format an die betroffene Person oder unmittelbar an einen anderen Verantwortlichen.

III.20.3 Binding Interpretations

VOM VERANTWORTLICHEN BEREITZUSTELLENDE DATEN:

- Gemäß dem Wortlaut „einem Verantwortlichen bereitgestellte Daten“:
  - → sind ausschließlich jene Daten gemeint, über die die betroffene Person Kontrolle hat und auf die sie selbst zugreift (z.B. Fotos und E-Mails).
  - → sind nicht die Nutzungsdaten und notwendigen Vertragsdaten gemeint.
- Demnach gilt insbesondere für **E-Mail-Dienste, Cloud-Dienste und Telekommunikationsdienste** Folgendes:
  - → Der Verantwortliche ist verpflichtet, diejenigen Daten bereitzustellen, die *ihm bereitgestellt worden sind*, und zwar zu einem beliebigen Zeitpunkt bis hin zum Zeitpunkt des Antrags. Dies dürften in erster Linie die **Daten der betroffenen Person in sozialen Medien** sein (Fotos, Kontakte und beliebige Daten, die von der betroffenen Person gespeichert wurden).
  - → Der Verantwortliche ist nicht verpflichtet, Daten bereitzustellen, die er von der betroffenen Person zur Erfüllung des Vertrags erhalten hat. Der Verantwortliche ist nicht verpflichtet, Daten bereitzustellen, die von der betroffenen Person zwischenzeitlich im Rahmen der Nutzung des Dienstes erzeugt wurden.

- Artikel 20 gilt auch im Beschäftigungskontext, beispielsweise für YAM-Daten (gemäß dem Recht auf Auskunft).
- Bei Fragen zur Anwendbarkeit dieses Artikels ist der DSB zu beteiligen.

FORMAT DER ÜBERMITTLUNG:

- Möglichkeit der direkten Übermittlung von einem zum anderen Verantwortlichen:
  → Bereits vorhandene interoperable Formate können verwendet werden.
- Übermittlung an die betroffene Person:
  → Es sollten gängige Formate wie z.B. CSV verwendet werden.

III.20.4 Fragebogen zur Compliance

- Gibt es ein Verfahren, einer betroffenen Person die Daten auf Verlangen in einem strukturierten, gängigen und maschinenlesbaren Format bereitzustellen oder diese an einen anderen Verantwortlichen zu übermitteln? [Ja]/[Nein]

- Gibt es ein Verfahren, nach dem die betroffene Person spätestens innerhalb eines Monats darüber informiert wird, weshalb der Verantwortliche in Bezug auf das Ersuchen der betroffenen Person nicht tätig geworden ist, sofern solche Gründe vorliegen? [Ja]/[Nein]

III.20.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe b: 20.000.000 EUR oder 4 % des gesamten weltweit erzielten Jahresumsatzes.

III.20.6 Best Practices und Vorlagen

Keine

ARTIKEL 21 WIDERSPRUCHSRECHT

III.21.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 21 – Widerspruchsrecht (Kapitel III – Rechte der betroffenen Person)
DSGVO ErwGr	69, 70
Querverweise	Artikel 6 Absatz 1; Artikel 13 Absatz 2 Buchstabe b; Artikel 14 Absatz 2 Buchstabe c; Artikel 15 Absatz 1 Buchstabe e; Artikel 17 Absatz 1 Buchstabe c; Artikel 18 Absatz 1 Buchstabe d; Artikel 89 Absatz 1
Zugehörige Unterlagen	Keine
BCRP Verweise	§ 5 Informationspflicht § 11 Automatisierte Einzelentscheidungen § 12 Die Verwendung personenbezogener Daten für Direktmarketingzwecke § 22 Widerspruchsrecht und Recht auf Löschung, Sperrung und Berichtigung

III.21.2 Zusammenfassung

Die betroffene Person hat das Recht, gegen die Verarbeitung ihrer Daten, die entweder aufgrund des öffentlichen Interesses oder zur Wahrung des berechtigten Interesses des Verantwortlichen erfolgt, Widerspruch einzulegen. Die Verarbeitung ist einzustellen, sofern die Interessen des Verantwortlichen nicht die Interessen der betroffenen Person überwiegen. Die betroffene Person kann zudem der Verarbeitung zum Zweck der Direktwerbung widersprechen.

III.21.3 Binding Interpretations

RECHT AUF WIDERSPRUCH GEGEN DIE VERARBEITUNG AUFGRUND EINES BERECHTIGTEN INTERESSES:

- **Der Widerspruch muss mit Gründen bezüglich der persönlichen/besonderen Situation begründet sein** und führt nicht unmittelbar zur Nichtigkeit der Rechtsgrundlage für die Verarbeitung, sondern vielmehr zu einer **Prüfung der Abwägung der jeweiligen Interessen.** Der Verantwortliche ist verpflichtet,

zwingende schutzwürdige Gründe für die Verarbeitung nachzuweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Ist er dazu nicht imstande, ist die Verarbeitung einzustellen.

RECHT AUF WIDERSPRUCH GEGEN DIE VERARBEITUNG IM ZUSAMMENHANG MIT DIREKTWERBUNG:

- Der Widerspruch wirkt sich unmittelbar und ohne weitere Interessenabwägung auf Direktwerbung auf der Grundlage von Profiling aus. Das bedeutet, dass der Verantwortliche verpflichtet ist, die personenbezogenen Daten unverzüglich zu löschen (siehe Artikel 17 Absatz 1 Buchstabe c).
- Direktmarketing bedeutet Werbung durch Nutzung von E-Mail, Anschrift und Telefonnummer anzustreben.

HINWEIS AN DIE BETROFFENE PERSON IN BEZUG AUF DAS WIDERSPRUCHSRECHT:

- Der Verantwortliche hat die betroffene Person auf die verschiedenen Widerspruchsrechte laut Artikel 21 spätestens zum Zeitpunkt der ersten Kommunikation hinzuweisen:
  - → Dies ist beispielsweise der Fall, wenn der erste Newsletter an den Empfänger verschickt wird.
  - → Siehe Informationen zu den Widerspruchsrechten im „One-Pager der Deutschen Telekom" und III.15.1.6.

AUSÜBUNG DES WIDERSPRUCHSRECHTS:

- Es ist ein Verfahren einzurichten, durch das sichergestellt wird, dass der Verantwortliche ein von der betroffenen Person mittels automatisierter Verfahren auf der Grundlage technischer Spezifikationen ausgeübtes Widerspruchsrecht umsetzen und verarbeiten kann.

III.21.4 Fragebogen zur Compliance

- Gibt es ein Verfahren, durch das bei Verarbeitung personenbezogener Daten auf der Grundlage der berechtigten Interessen des Verantwortlichen (Artikel 6 Absatz 1 Buchstabe f) die berechtigten vorrangigen Interessen des Verantwortlichen dokumentiert werden? [Ja]/[Nein]
- Können die berechtigten Interessen des Verantwortlichen im Falle eines Widerspruchs belegt werden? [Ja]/[Nein]
- Werden Personen in verständlicher und von anderen Informationen getrennter Form bei der ersten Kommunikation auf ihr Widerspruchsrecht hingewiesen (z.B. durch Erklärungen und Policies)? [Ja]/[Nein]
- Gibt es ein Verfahren, durch das sichergestellt wird, dass die Verarbeitung von Daten unverzüglich eingestellt werden kann, sobald die betroffene Person der Direktwerbung bzw. der Direktwerbung auf der Grundlage von Profiling widerspricht? [Ja]/[Nein]
- Gibt es ein Verfahren, das es der betroffenen Person ermöglicht, ihr Widerspruchsrecht mittels automatisierter Verfahren auf der Grundlage technischer Spezifikationen, auszuüben? [Ja]/[Nein]

III.21.5 Sanktionen

Keine

III.21.6 Best Practices und Vorlagen

- Siehe III.15.6

ARTIKEL 22 AUTOMATISIERTE ENTSCHEIDUNGEN IM EINZELFALL EINSCHLIEẞLICH PROFILING

III.22.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 22 – Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Kapitel III – Rechte der betroffenen Person)
DSGVO ErwGr	69, 70, 71, 72
Querverweise	Artikel 4 Absatz 4; Artikel 12 bis 15; Artikel 21; Artikel 35
Zugehörige Unterlagen	Keine
BCRP Verweise	§ 11 Automatisierte Einzelentscheidungen

III.22.2 Zusammenfassung

Einzelpersonen haben das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder in ähnlicher Weise erhebliche Auswirkungen auf sie hat. Es gibt einige Ausnahmen, beispielsweise wenn die auf Profiling beruhende Entscheidung für den Abschluss eines Vertrags mit der betroffenen Person erforderlich ist.

III.22.3 Binding Interpretations

UMFANG:

- Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung beruhen und sich auf die Bewertung *persönlicher Aspekte* der betroffenen Person stützen (§ 11 Buchstabe a BCRP):
  - → Beispiele sind eine automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen.
- Profiling ist ein Beispiel einer automatisierten Entscheidungsfindung, das ausdrücklich in Artikel 22 genannt ist.
  - → Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel (siehe Artikel 4 Absatz 4)
  - → Beurteilung bei Kreditauskunfteien, wenn diese ausschließlich mittels automatisierter Verfahren ohne menschliches Eingreifen erfolgt.

INFORMATIONEN ÜBER DIE AUTOMATISIERTE ENTSCHEIDUNGSFINDUNG:

- Übermittlung von konkreten Informationen und Erläuterungen zur Entscheidung: Die wesentlichen Gründe für die Entscheidung müssen nicht nur auf Verlangen erläutert werden, sodass die betroffene Person in der Lage ist, ihren eigenen Standpunkt darzulegen.
- Es müssen sinnvolle Informationen zur Logik, nach der die automatische Entscheidung erfolgt, sowie zur Bedeutung und den voraussichtlichen Folgen bereitgestellt werden:
  → Dies kann in einer Datenschutzpolicy oder in Form einer Antwort auf das Verlangen der betroffenen Person nach Auskunft zu ihren Daten erfolgen.
- Sofern die sachliche Notwendigkeit zur Vornahme automatisierter Entscheidungen besteht, ist die betroffene Person unverzüglich über das Ergebnis der automatisierten Entscheidung zu informieren und ihr die Möglichkeit zur Stellungnahme zu geben (§ 11 Buchstabe a BCRP).

BESONDERE ANFORDERUNGEN AN DAS PROFILING:

- Wenn die Verarbeitung personenbezogener Daten zum Zweck des Profiling erfolgt, muss sichergestellt werden, dass geeignete Garantien bestehen:
  → Anspruch auf direktes Eingreifen einer Person, Anfechtung der Entscheidung u.a.
- Für das Profiling müssen geeignete mathematische oder statistische Verfahren verwendet werden.
- Es müssen technische und organisatorische Maßnahmen getroffen werden, mit denen unrichtige personenbezogene Daten korrigiert werden können und das Risiko von Fehlern minimiert werden kann.
  → Dies ist beispielsweise durch eine Plausibilitätskontrolle möglich.
- Bei der Sicherung personenbezogener Daten ist den potenziellen Risiken für die Interessen und Rechte der betroffenen Person Rechnung zu tragen; diskriminierende Auswirkungen auf die betroffene Person sind zu verhindern.

ANWENDUNG DES PSA-VERFAHRENS VOR DER AUTOMATISIERTEN ENTSCHEIDUNGSFINDUNG IM EINZELFALL:

- Eine Datenschutz-Folgenabschätzung ist erforderlich, wenn eine systematische und eingehende Bewertung der persönlichen Aspekte natürlicher Personen, die auf Profiling beruht, beabsichtigt ist und darauf Entscheidungen gründen, die in Bezug auf die Person rechtliche Wirkungen entfalten oder erhebliche Auswirkungen auf sie haben. Das PSA-Verfahren erfüllt diese Anforderung (Kategorie A des PSA-Verfahrens).
- Widerspruchsrecht (siehe Artikel 21 Absatz 3)

III.22.4 Fragebogen zur Compliance

- Falls es Anwendungsfälle für eine automatisierte Entscheidungsfindung im Einzelfall einschließlich Profiling gibt:
  - Ist es ausgeschlossen, dass ein Kind einer automatisierten Entscheidung unterworfen ist? [Ja]/[Nein]

- Gibt es eine Rechtsgrundlage (notwendig für Vertrag, aufgrund von Rechtsvorschriften der Union oder eines Mitgliedstaates zulässig oder ausdrückliche Einwilligung der betroffenen Person)? [Ja]/[Nein]
- Gibt es eine Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten (Verarbeitung dieser Daten für einen oder mehrere festgelegte Zwecke mit ausdrücklicher Einwilligung der betroffenen Person, außer wenn das Verbot nach Unionsrecht oder dem Recht eines Mitgliedsstaates nicht von der betroffenen Person aufgehoben werden kann)? [Ja]/[Nein]
- Werden für das Profiling geeignete mathematische oder statistische Verfahren verwendet? [Ja]/[Nein]
- Sind geeignete Maßnahmen zum Schutz der Rechte der betroffenen Person getroffen worden, z.B.:
    - → Erhält die betroffene Person konkrete Informationen und Erläuterungen zur Entscheidung? [Ja]/[Nein]
    - → Ist das Recht der betroffenen Person gewährleistet, die Entscheidung anzufechten, ihren eigenen Standpunkt darzulegen und ein direktes Eingreifen einer Person auf Seiten des Verantwortlichen zu verlangen? [Ja]/[Nein]
    - → Sind die ergriffenen TOM angemessen, um die personenbezogenen Daten zu sichern und das Risiko von Fehlern zu minimieren? [Ja]/[Nein]

III.22.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe b: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes.

III.22.6 Best Practices und Vorlagen

Keine

KAPITEL IV – VERANTWORTLICHER UND AUFTRAGSVERARBEITER

Artikel 24 bis 43

Dieses Kapitel ist in fünf Abschnitte unterteilt. Kapitel IV Abschnitt 1 regelt die allgemeinen Pflichten des Verantwortlichen und des Auftragsverarbeiters. Mit der DSGVO werden Anforderungen für ein Verzeichnis von Verarbeitungstätigkeiten und Kategorien von Verarbeitungstätigkeiten eingeführt. Der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen wird als wesentlicher Aspekt der Verarbeitung personenbezogener Daten beschrieben.

Abschnitt 2 enthält die Anforderungen für die Sicherheit personenbezogener Daten sowie die Verfahren, die bei Verletzung des Schutzes personenbezogener Daten eingehalten werden müssen, sei es die Meldung an die Aufsichtsbehörde oder die Benachrichtigung der betroffenen Person.

In Abschnitt 3 ist festgelegt, wann eine Datenschutz-Folgenabschätzung durchzuführen ist und in welchen Fällen der Verantwortliche vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde zu konsultieren hat.

Abschnitt 4 regelt die Stellung, Aufgaben und Zuständigkeiten des Datenschutzbeauftragten (DSB). Abschnitt 5 schließlich befasst sich mit den Instrumenten 'Verhaltensregeln' und 'Zertifizierung', mit denen der Nachweis für die Einhaltung der DSGVO erbracht werden kann.

ARTIKEL 24 VERANTWORTUNG DES FÜR DIE VERARBEITUNG VERANTWORTLICHEN

IV.24.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 24 – Verantwortung des für die Verarbeitung Verantwortlichen (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	74–77
Querverweise	Artikel 40; 42
Zugehörige Unterlagen	Keine
BCRP Verweise	§ 20 Datensicherheit – Technische und organisatorische Maßnahmen

IV.24.2 Zusammenfassung

Der Verantwortliche stellt durch geeignete technische und organisatorische Maßnahmen – häufig zum Beispiel durch eine Datenschutz-Policy – sicher, dass die Verarbeitung gemäß der DSGVO erfolgt und dies entsprechend nachweisbar ist. Die Erfüllung der Pflichten des Verantwortlichen kann durch die Einhaltung von Verhaltensregeln oder einen Zertifizierungsmechanismus nachgewiesen werden.

IV.24.3 Binding Interpretations

UMSETZUNG UND DOKUMENTATION DER TOM:

- Geeignete technische und organisatorische Maßnahmen und Datenschutz-Policies sind umzusetzen und zu dokumentieren. Innerhalb des Konzerns Deutsche Telekom werden diese Anforderungen durch das PSA-Verfahren und die Anwendung von standardisierten Verträgen über die Auftragsdatenverarbeitung (CDPA), die von Group Privacy (GPR) bereitgestellt werden, erfüllt.
- In Datenschutz-Policies werden die Anforderungen und Regeln für den Datenschutz festgelegt. Diese sind in den folgenden Instrumenten bzw. Dokumenten enthalten:
  - → PSA-Verfahren
  - → Andere Dokumentation, z.B. Regelungen in YAM, Datenschutzvorschriften in Arbeitsverträgen
- Die Einhaltung der DSGVO kann durch die Einhaltung der BCRP und der Binding Interpretations zur DSGVO nachgewiesen werden.

ZERTIFIZIERUNGSMECHANISMUS:

- Soweit vorhanden sind Zertifizierungsmechanismen zu nutzen.

PSA-VERFAHREN:

- Beim PSA-Verfahren handelt es sich um einen EU-weiten Standard innerhalb des Konzerns Deutsche Telekom, der als Informationssicherheits-Managementsystem zertifiziert wurde, das die Anforderungen der Norm ISO/IEC 27001: 2013 erfüllt. Mithilfe des PSA-Verfahrens kann sichergestellt werden, dass die Anforderungen gemäß Artikel 24 und § 20 BCRP erfüllt und die jeweils geforderten Aufzeichnungen geführt werden.

IV.24.4 Fragebogen zur Compliance

- Wird bei allen wichtigen Projekten und Systemen ein PSA-Verfahren durchgeführt? [Ja]/[Nein]
- Gibt es ein Verfahren, das vor der Beauftragung eines Dritten mit Verarbeitungstätigkeiten den Abschluss einer Datenverarbeitungsvereinbarung und die Umsetzung der jeweiligen TOM sicherstellt? [Ja]/[Nein]
- Erfolgt eine hinreichende Dokumentation, damit die Einhaltung der Verordnung nachgewiesen werden kann? [Ja]/[Nein]
- Gibt es ein Verfahren, mit dem die Einhaltung der BCRP und der Binding Interpretations überprüft werden kann? [Ja]/[Nein]
- Gibt es Zertifizierungen? [Ja]/[Nein]

IV.24.5 Sanktionen

Keine

IV.24.6 Best Practices und Vorlagen

Keine

ARTIKEL 25 DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

IV.25.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	78
Querverweise	Artikel 4 Absatz 5; Artikel 47 Absatz 2 Buchstabe d
Zugehörige Unterlagen	Empfehlung der Kommission vom 10. Oktober 2014 über das Muster für die Datenschutz-Folgenabschätzung für intelligente Stromnetze und intelligente Messsysteme (2014/724/EU) Artikel-29-Arbeitsgruppe: Arbeitspapier 223, „Stellungnahme 8/2014 zu den jüngsten Entwicklungen in Bezug auf das Internet der Dinge“
BCRP Verweise	§ 20 Datensicherheit – Technische und organisatorische Maßnahmen

IV.25.2 Zusammenfassung

Mit Artikel 25 wird der Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen eingeführt. Nach diesem Grundsatz hat der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung während des Lebenszyklus einer Dienstleistung, eines Produkts oder einer anderen Verarbeitungstätigkeit geeignete technische und organisatorische Maßnahmen (z.B. Pseudonymisierung) zu treffen, die darauf ausgelegt sind, die Datenschutzgrundsätze umzusetzen. Der Verantwortliche ist verpflichtet, durch datenschutzfreundliche Voreinstellungen, technische und organisatorische Maßnahmen (TOM) umzusetzen, durch die sichergestellt werden kann, dass ausschließlich die für den jeweiligen Zweck erforderlichen Daten verarbeitet werden.

IV.25.3 Binding Interpretations

VERPFLICHTENDE UMSETZUNG VON TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN:

- Jedes Unternehmen des Konzerns Deutsche Telekom ist dazu verpflichtet, das Konzept „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ umzusetzen.
- Der Datenschutz darf nicht nur in den letzten Phasen der Produkt- oder Dienstleistungskonfiguration berücksichtigt werden, sondern muss von Anfang an und während des gesamten Lebenszyklus berücksichtigt werden.
- Die Aufsichtsbehörde berücksichtigt bei der Entscheidung, ob und in welcher Höhe eine Geldbuße verhängt wird, in welchem Maße TOM nach Artikel 25 getroffen worden sind (siehe Artikel 83 Absatz 2 Buchstabe d).
- Beispielsweise: Keine bereits angeklickten Inhaltsboxen bezüglich datenschutzfreundliche Voreinstellungen.

PSA-VERFAHREN:

- Damit der Konzern die DSGVO jederzeit einhält, ist das PSA-Verfahren in der gültigen, von der Abteilung GPR bereitgestellten Fassung (http://drc.telekom.de/en/sec/privacy-security-assessment) in jedem zum Konzern Deutsche Telekom zugehörigen Unternehmen umzusetzen (siehe auch IV.25.6).
- Die Anforderungen an den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen werden insbesondere im “Initial Consultation Guide" und in den Datenschutzanforderungen des PSA-Verfahrens behandelt. Das PSA-Verfahren ist ohne den „Initial Consultation Guide“, die Rahmenbestimmungen und Schwerpunktüberprüfungen nicht ausreichend.

IV.25.4 Fragebogen zur Compliance

- Wurde das PSA-Verfahren in der gültigen, von GPR bereitgestellten Fassung umgesetzt? [Ja]/[Nein]

IV.25.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

IV.25.6 Best Practices und Vorlagen

- Datenschutzanforderungen der Abteilung GPR/Initial Consultation Guide (ICG 5): https://psa-portal.telekom.de

ARTIKEL 26 GEMEINSAM FÜR DIE VERARBEITUNG VERANTWORTLICHE

IV.26.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 26 – Gemeinsam für die Verarbeitung Verantwortliche (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	79
Querverweise	Artikel 4 Absatz 7; Artikel 36 Absatz 3 Buchstabe a
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 169, „Stellungnahme 1/2010 zu den Konzepten ‚Verantwortlicher' und ‚Auftragsverarbeiter'" Information Commissioner's Office (ICO) „Data Controllers and Data Processors 20140506 Version: 1.0" Arbeitsbericht der Ad-Hoc-Arbeitsgruppe „Konzerninterner Datentransfer", 11.01.2005, Regierungspräsidium Darmstadt, Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich
BCRP Verweise	§ 27 Verantwortung für die Datenverarbeitung Teil 7 Definitionen und Begriffe

IV.26.2 Zusammenfassung

In diesem Artikel wird definiert, was es bedeutet, gemeinsam für die Verarbeitung verantwortlich zu sein, und welche Bedingungen für eine solche gemeinsame Verarbeitung gelten.

IV.26.3 Binding Interpretations

DEFINITION DES BEGRIFFS „GEMEINSAM FÜR DIE VERARBEITUNG VERANTWORTLICHE":

- Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der Verarbeitung und die entsprechenden Mittel fest, so sind sie gemeinsam Verantwortliche.

PFLICHTEN GEMEINSAM VERANTWORTLICHER:

- Gemeinsam Verantwortliche sind beide für die Datenverarbeitungstätigkeiten verantwortlich.

- Die fehlende Aufteilung der jeweiligen Pflichten kann höhere Geldbußen nach sich ziehen (siehe Artikel 83 Absatz 2 Buchstabe d).

VEREINBARUNGEN ZU DEN PFLICHTEN:

- Die jeweiligen Pflichten sind gemäß Artikel 26 in eindeutiger Form in einer Vereinbarung festzulegen.
- Empfehlung für den Inhalt dieser Vereinbarung:
  - → Klare Beschreibung der Pflichten und Zuständigkeiten, insbesondere, wer der Pflicht zur klaren und transparenten Information der betroffenen Person gemäß Artikel 13 und 14 nachkommt
  - → Obligatorische Koordination mit dem DSB des Konzernunternehmens bei Verträgen mit gemeinsamer Verantwortung für die Datenverarbeitung
- Die betroffene Person wird über den wesentlichen Inhalt der Vereinbarung informiert.

IV.26.4 Fragebogen zur Compliance

- Falls Ihr Unternehmen als Verantwortlicher mit einem anderen Verantwortlichen im Zusammenhang mit denselben Verarbeitungstätigkeiten zusammenarbeitet, besteht zwischen diesen beiden Verantwortlichen eine Vereinbarung gemäß Artikel 26 DSGVO? [Ja]/[Nein]

IV.26.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes

IV.26.6 Best Practices und Vorlagen

Keine

ARTIKEL 28 AUFTRAGSVERARBEITER

ARTIKEL 29 VERARBEITUNG UNTER DER AUFSICHT DES VERANTWORTLICHEN ODER DES AUFTRAGSVERARBEITERS

IV.28., 29.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 28 – Auftragsverarbeiter (Kapitel IV – Verantwortlicher und Auftragsverarbeiter) Artikel 29 – Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	81
Querverweise	Artikel 4; 24; 26; 27; Artikel 30 Absatz 2; Artikel 31; 32; Artikel 33 Absatz 2; Artikel 37 bis 40; Artikel 42; Artikel 44 bis 49; Artikel 58; 77; 79; 82; 83
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 169, „Stellungnahme 1/2010 zu den Konzepten ‚Verantwortlicher' und ‚Auftragsverarbeiter'"
BCRP Verweise	§ 18 Datenverarbeitung im Auftrag

IV.28., 29.2 Zusammenfassung

Artikel 28 regelt die Anforderungen bei einer Verarbeitung im Auftrag eines Verantwortlichen. Darüber hinaus enthält dieser Artikel besondere Bestimmungen für den Fall, dass der Auftragsverarbeiter einen weiteren Auftragsverarbeiter beauftragen will.

In Artikel 29 ist festgeschrieben, dass der Auftragsverarbeiter nach Weisung des Verantwortlichen zu handeln hat, es sei denn, dass er nach Unionsrecht oder dem Recht eines Mitgliedstaates zur Verarbeitung verpflichtet ist.

IV.28., 29.3 Binding Interpretations

FORM EINES VERTRAGS ÜBER DIE AUFTRAGSVERARBEITUNG:

- **Verarbeitung im Auftrag des Verantwortlichen:** Diese unterliegt einem schriftlichen Vertrag – Artikel 28 Absatz 9 –, dem Vertrag über Auftragsverarbeitung (siehe IV.28, 29.6). Diese Anforderung

ist auch bei Verträgen in elektronischer Form erfüllt; eine persönliche Unterschrift ist nicht erforderlich. Zur Erleichterung eines späteren Nachweises werden digitale Unterschriften wie bei DocuSign oder PDF-Unterschriften empfohlen.

- **Verhaltensregeln:** Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Einhaltung der Pflichten des Verantwortlichen nachzuweisen.
  → **Zu prüfen:** Bis zum Inkrafttreten der DSGVO ist jegliche Verarbeitung personenbezogener Daten innerhalb des Konzerns Deutsche Telekom in Einklang mit der Verordnung zu bringen (siehe Artikel 99). Daher sind bestehende Verträge über Auftragsverarbeitung daraufhin zu prüfen, ob sie den Anforderungen gemäß Artikel 28 entsprechen (siehe IV.28, 29.6).

INHALT EINES VERTRAGS ÜBER DIE AUFTRAGSVERARBEITUNG:

- **Auswahl des Auftragsverarbeiters:** Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so beauftragt dieser nur Auftragsverarbeiter, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen ergriffen werden:
  - Die technischen und organisatorischen Maßnahmen (TOM) haben durchweg hohen Datenschutzanforderungen zu entsprechen. In Bezug auf interne Systeme der Deutschen Telekom ist das PSA-Verfahren anzuwenden. Die im Rahmen des PSA-Verfahrens durchgeführten Kontrollen sind von dem Bereich der Deutschen Telekom vorzunehmen, der die personenbezogenen Daten tatsächlich verarbeitet. Externe Systeme, mit denen Daten von Unternehmen der Deutschen Telekom verarbeitet werden, haben die PSA-Anforderungen zu erfüllen.
  - Die Einhaltung der vertraglich vereinbarten TOM ist unverzüglich nach Vertragsschluss *und vor Beginn* der eigentlichen Verarbeitung zu prüfen. Sofern es sinnvoll und angemessen erscheint, erklärt der Auftragsverarbeiter durch eine „Selbstauskunft", dass er die Datenschutzbestimmungen einhält, und bestätigt dies im sogenannten SOC-Dokument (https://drc.telekom.de/de/privacy/service/adv-kontrollen—was-ist-das/112718) gegenüber dem beauftragenden Konzernunternehmen. In allen anderen Fällen ist ein Audit durchzuführen.
- **Unterauftragsverarbeiter:** Bei der Beauftragung eines Unterauftragsverarbeiters hat der Auftragsverarbeiter folgende Bestimmungen einzuhalten:
  - Der Auftragsverarbeiter benötigt entweder die vorherige spezifische Genehmigung des Verantwortlichen oder eine allgemeine schriftliche Genehmigung, die auch in elektronischer Form erfolgen kann. Im letzteren Fall informiert der Auftragsverarbeiter den Verantwortlichen über die beabsichtigte Beauftragung von Unterauftragsverarbeitern, sodass der Verantwortliche Einspruch dagegen erheben kann. Der Verantwortliche hat zu entscheiden, ob eine vorherige Genehmigung für die Beauftragung von Unterauftragsverarbeitern erforderlich ist oder ob eine allgemeine Genehmigung nach den Anforderungen gemäß Artikel 28 erteilt wird. Der Auftragsverarbeiter als verarbeitende Organisation hat die Genehmigung für die Beauftragung von Unterauftragsverarbeitern beim Verantwortlichen einzuholen. Entsprechende Klauseln sind in den Vertrag aufzunehmen (siehe 28, 29.6).
  - Der Auftragsverarbeiter hat einem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten aufzuerlegen, die im Vertrag über die Auftragsverarbeitung enthalten sind.

Sollte dies in bestimmten Fällen – selbst nach Konsultation des zuständigen DSB – nicht möglich sein, können Standardvertragsklauseln laut Artikel 28 Absatz 7 oder andere in Artikel 28 Absatz 6 aufgeführte Mechanismen eingesetzt werden.

- **Haftung:** Personenbezogene Daten dürfen nur von einer im Auftrag des Verantwortlichen oder des Auftragsverarbeiters handelnden Person entsprechend den dokumentierten Weisungen des Verantwortlichen verarbeitet werden.
  - Bei Nichtbeachtung der Weisungen des Verantwortlichen, beispielsweise wenn Daten zu anderen Zwecken verarbeitet werden, wird der Auftragsverarbeiter als in Bezug auf diese Verarbeitung Verantwortlicher angesehen und entsprechend haftbar gemacht.
  - Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, bleibt der Erstauftragsverarbeiter vollumfänglich haftbar.

  → VORLAGE: Weitere Einzelheiten zu den Anforderungen an den Vertrag über die Auftragsverarbeitung sind in der Vorlage unter IV.28, 29.6 zu finden.

IV.28., 29.4 Fragebogen zur Compliance

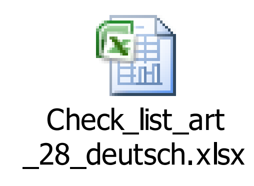
- Verantwortlicher und Auftragsverarbeiter: Prüfen Sie den bestehenden Vertrag über die Auftragsverarbeitung auf Einhaltung der DSGVO? [Ja]/[Nein]
- Verantwortlicher und Auftragsverarbeiter: Unterliegt jegliche Datenverarbeitung im Auftrag des Verantwortlichen einem schriftlichen Vertrag (Vertrag über die Auftragsverarbeitung, Artikel 28 Absatz 9)? [Ja]/[Nein]
- Verantwortlicher: Ist gewährleistet, dass der Auftragsverarbeiter hinreichend Garantien dafür bietet, dass geeignete TOM ergriffen werden (z.B. Zertifizierung)? [Ja]/[Nein]
- Verantwortlicher: Prüfen Sie erstmalig nach Vertragsschluss und vor Beginn der eigentlichen Verarbeitung, ob die vertraglich vereinbarten TOM tatsächlich ergriffen worden sind? [Ja]/[Nein]
- Verantwortlicher und Auftragsverarbeiter: Werden die Verpflichtungen der Parteien und die Haftungsfragen eindeutig im Vertrag festgelegt? [Ja]/[Nein]
- Verantwortlicher und Auftragsverarbeiter: Wird die obligatorische Dokumentation tatsächlich vorgenommen? [Ja]/[Nein]
- Auftragsverarbeiter: Liegt Ihnen eine schriftliche Genehmigung des Verantwortlichen für die Beauftragung aller beauftragten Unterauftragsverarbeiter vor? [Ja]/[Nein]
- Auftragsverarbeiter: Informieren Sie den Verantwortlichen bei Vorliegen einer gesonderten oder allgemeinen schriftlichen Genehmigung des Verantwortlichen zur Beauftragung von Unterauftragsverarbeitern über jede beabsichtigte Änderung bei den Unterauftragsverarbeitern? [Ja]/[Nein]
- Auftragsverarbeiter: Sollten Sie mit der vorherigen schriftlichen Genehmigung des Verantwortlichen Unterauftragsverarbeiter beauftragen, haben Sie vor Beginn der eigentlichen Datenverarbeitung (und im Anschluss daran in regelmäßigen Zeitabständen) überprüft, ob diese Unterauftragsverarbeiter ihren Verpflichtungen – insbesondere Beachtung der vertraglich vereinbarten TOM – nachkommen? Dokumentieren Sie die Ergebnisse dieser Überprüfungen? [Ja]/[Nein]
- Auftragsverarbeiter: Verarbeiten Sie Daten ausschließlich gemäß den Bestimmungen des Vertrags und den Weisungen des Verantwortlichen, sofern Sie nicht nach Unionsrecht oder dem Recht einem Mitgliedstaates anderweitig verpflichtet sind? [Ja]/[Nein]

IV.28., 29.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

IV.28., 29.6 Best Practices und Vorlagen

- Checkliste:



ARTIKEL 30 VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

IV.30.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 30 – Verzeichnis von Verarbeitungstätigkeiten (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	82
Querverweise	Artikel 5 Absatz 2; Artikel 24; Artikel 28 bis 33; Artikel 49 Absatz 6
Zugehörige Unterlagen	Keine
BCRP Verweise	Keine

IV.30.2 Zusammenfassung

Sowohl der Verantwortliche als auch der Auftragsverarbeiter haben Verzeichnisse zu führen. Der Verantwortliche führt ein Verzeichnis von Verarbeitungstätigkeiten, das er der Aufsichtsbehörde auf Verlangen zur Verfügung stellt. Der Auftragsverarbeiter führt ein Verzeichnis zu den Kategorien der Verarbeitung. Die inhaltlichen Anforderungen beider Verzeichnisse unterscheiden sich voneinander.

IV.30.3 Binding Interpretations

PFLICHT DES VERANTWORTLICHEN EIN VERZEICHNIS ZU FÜHREN:

- Der Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten, für die er verantwortlich ist. Dieses Verzeichnis enthält verschiedene Informationen, darunter Kontaktdaten, den Zweck der Verarbeitung, Informationen zur Übermittlung in Drittländer und ggf. Fristen für die Löschung und TOM (siehe Artikel 30 Absatz 1).
- Die Anforderungen gemäß Artikel 30 Absatz 1 werden durch die Verwendung der Software CAPE erfüllt.

PFLICHT DES AUFTRAGSVERARBEITERS EIN VERZEICHNIS ZU FÜHREN:

- Der Auftragsverarbeiter führt ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das u.a. die Kontaktdaten des Auftragsverarbeiters und ggf. Angaben zur Übermittlung in Drittländer enthält.

IV.30.4 Fragebogen zur Compliance

- Verantwortlicher und Auftragsverarbeiter: Gibt es einen Überblick über Ihre Verarbeitungstätigkeiten? [Ja]/[Nein]
- Verantwortlicher: Wird ein Verzeichnis mithilfe von CAPE geführt? [Ja]/[Nein]
    - Falls nein, enthält ihr Verzeichnis, sämtliche erforderlichen Informationen laut Artikel 30 Absatz 1? [Ja]/[Nein]
    - Wurde in Erwägung gezogen, das Tool „CAPE" zu verwenden, das Teil des Compliance-Management-Systems des Konzerns Deutsche Telekom und als solches Teil der Zertifizierung des Konzerns Deutsche Telekom nach PS 980 ist? [Ja]/[Nein]
- Auftragsverarbeiter: Sind Sie in der Lage, gemäß Artikel 30 Absatz 2 ein Verzeichnis zu Ihren Tätigkeiten als Auftragsverarbeiter zu führen? [Ja]/[Nein]

IV.30.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

IV.30.6 Best Practices und Vorlagen

Keine

ARTIKEL 32 SICHERHEIT DER VERARBEITUNG

IV.32.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 32 – Sicherheit der Verarbeitung (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	83
Querverweise	Artikel 4 Absatz 5; Artikel 5 Absatz 1 Buchstabe f und Absatz 2; Artikel 24 Absatz 1; Artikel 25 Absatz 1 und 2; Artikel 28 Absatz 1 und Absatz 3 Buchstabe c; Artikel 30 Absatz 1 Buchstabe g und Absatz 2 Buchstabe d; Artikel 34 Absatz 3 Buchstabe a; Artikel 35 Absatz 7 Buchstabe d; Artikel 40 Absatz 2 Buchstabe h; Artikel 42; 44
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 216, „Stellungnahme 05/2014 zu Anonymisierungsmethoden“
BCRP Verweise	§ 20 Datensicherheit – Technische und organisatorische Maßnahmen

IV.32.2 Zusammenfassung

Verantwortliche und Auftragsverarbeiter haben geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

IV.32.3 Binding Interpretations

STANDARDMÄSSIGE TOM UND DAS STANDARD-PSA-VERFAHREN BEI UNTERNEHMEN DES KONZERNS DEUTSCHE TELEKOM:

- Die wesentlichen in der DSGVO genannten Zielvorgaben der IT-Sicherheit, beispielsweise Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, sind vollumfänglich von den standardmäßigen TOM der Telekom (§ 20 BCRP) und den entsprechenden Sicherheitsanforderungen gemäß dem PSA-Verfahren abgedeckt.
- Um der Rechenschaftspflicht jederzeit zu genügen, sind gemäß DSGVO verpflichtend Risikobewertungen vorzunehmen, das Schutzniveau ist festzulegen und Maßnahmen zur Risikominderung sind zu dokumentieren. Durch das PSA-Verfahren des Konzerns Deutsche Telekom sind diese Pflichten vollumfänglich erfüllt.

Damit die Einhaltung der DSGVO sämtlicher darin festgelegter Sicherheitsanforderungen jederzeit gewährleistet ist, ist das PSA-Verfahren in der gültigen, von GPR bereitgestellten Fassung (http://drc.telekom.de/en/sec/privacy-security-assessment) in jedem zum Konzern Deutsche Telekom zugehörigen Unternehmen umzusetzen.

SICHERHEITSVERPFLICHTUNGEN DES AUFTRAGSVERARBEITERS:

- Haftung: Wenn Unternehmen der Deutschen Telekom als Auftragsverarbeiter tätig sind (z.B. T-Systems), sind sie – ungeachtet der vertraglichen Verpflichtungen – gleichermaßen für die Sicherheit der Verarbeitung und die Einhaltung der DSGVO verantwortlich.
- Externer Verantwortlicher: Erfolgt die Verarbeitung im Auftrag eines externen Verantwortlichen, der nicht zum Konzern Deutsche Telekom gehört, kann der Nachweis für die Einhaltung der DSGVO statt durch PSA durch eine Zertifizierung erbracht werden.

IV.32.4 Fragebogen zur Compliance

- Wurde das PSA-Verfahren in der gültigen, von GPR bereitgestellten Fassung umgesetzt? (Insbesondere die Kategorisierung und Erstberatung (Initial Consultation) – ICG 5 –, da diese PSA-Tools für die Bewertung des Datenschutzrisikos herangezogen werden.) [Ja]/[Nein]
- Werden PSA-Überprüfungen stichprobenartig durchgeführt, um festzustellen, ob die Dokumentation und Kategorisierung im PSA-Verfahren korrekt vorgenommen wird? [Ja]/[Nein]

IV.32.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

IV.32.6 Best Practices und Vorlagen

- PSA: https://drc.telekom.de/de/sec/privacy-security-assessment
- PSA-Portal: https://psa-portal.telekom.de/intranet-ui/

ARTIKEL 33 MELDUNG VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN AN DIE AUFSICHTSBEHÖRDE

ARTIKEL 34 BENACHRICHTIGUNG DER VON EINER VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN BETROFFENEN PERSON

IV.33, 34.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Kapitel IV – Verantwortlicher und Auftragsverarbeiter) Artikel 34 – Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	85 bis 88
Querverweise	Artikel 4 Absatz 12
Zugehörige Unterlagen	Artikel-29-Arbeitsgruppe: Arbeitspapier 213, „Stellungnahme 03/2014 zur Meldung von Verletzungen des Schutzes personenbezogener Daten“
BCRP Verweise	§ 23 Recht auf Klärung, Stellungnahme und Abhilfe § 30 Informationspflicht bei Verstößen *nur konzernintern, nicht gegenüber Aufsichtsbehörde*

IV.33, 34.2 Zusammenfassung

Im Falle einer Verletzung des Schutzes personenbezogener Daten ist die zuständige Aufsichtsbehörde unverzüglich zu informieren. Der Verantwortliche muss die betroffene Person über die Verletzung benachrichtigen, sofern sich aus der Verletzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person ergibt.

IV.33, 34.3 Binding Interpretations

VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN:

- **Verletzung der Sicherheit:** Gemäß Artikel 4 Absatz 12 stellt die Verletzung des Schutzes personenbezogener Daten eine Verletzung der Sicherheit dar, die – unbeabsichtigt oder

unrechtmäßig – zu Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von übermittelten, gespeicherten oder sonstwie verarbeiteten personenbezogenen Daten führt bzw. unbefugten Zugang zu solchen Daten ermöglicht.

- **Meldung:** Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, hat er diese dem Verantwortlichen unverzüglich zu melden. Dem Verantwortlichen bzw. Auftragsverarbeiter wird eine Verletzung des Schutzes personenbezogener Daten bekannt, sobald er die Fakten kennt, die eine solche Verletzung nach der obigen Definition darstellen. Ein bloßer Verdacht ist nicht ausreichend.

PFLICHT ZUR BENACHRICHTIGUNG DER AUFSICHTSBEHÖRDE:

- Nachdem er von einer Datenschutzverletzung Kenntnis erlangt hat, muss der Verantwortliche beurteilen, ob diese Verletzung voraussichtlich zu einem **Risiko bzw. hohen Risiko** für die Rechte und Freiheiten von betroffenen Personen führt (siehe Artikel 33 Absatz 1 und Artikel 34).
  - Anzeichen für ein bestehendes Risiko:
    - → Verlust der Kontrolle der betroffenen Person über ihre personenbezogenen Daten; Verarbeitung besonderer Kategorien von Daten, automatisierte Entscheidungsfindung einschließlich Profiling; Verarbeitung von Daten schutzbedürftiger betroffener Personen; Verarbeitung in großem Umfang.
  - Anzeichen für ein bestehendes hohes Risiko:
    - → Systematisches und eingehendes automatisiertes Profiling; umfangreiche Verarbeitung besonderer Kategorien von Daten; systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
  - In folgenden Fällen hat die Datenschutzverletzung **voraussichtlich kein** Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge:
    - → Daten sind verschlüsselt; der Verantwortliche verarbeitet ausschließlich „anonymisierte Daten" (diese fallen nicht unter die DSGVO); die Verletzung ist von sehr geringfügigem Ausmaß und betrifft lediglich unkritische Informationen über eine kleine Gruppe von Menschen. In diesen Fällen muss die Aufsichtsbehörde nicht informiert werden (siehe Artikel 33 Absatz 1).
- Die Meldung gegenüber der zuständigen Aufsichtsbehörde nimmt der Verantwortliche – der DSB oder der Verantwortliche unter Hinzuziehung des DSB – vor. Grundsätzlich ist die Aufsichtsbehörde des Mitgliedstaats zuständig in dem der Verantwortliche niedergelassen ist (Ausnahmen siehe Abschnitt IV.33.6 „Prozessmodell Incident Management"). Welche Inhalte in die Meldung gehören, ist der Vorlage „Meldung bei Datenschutzverletzungen gemäß DSGVO" zu entnehmen (siehe IV.33.6).
- Die Meldung an die Aufsichtsbehörde hat unverzüglich und möglichst binnen 72 Stunden zu erfolgen. Sollte die Meldung erst später erfolgen, ist ihr eine Begründung für die Verzögerung beizufügen.
- Wenn der Verantwortliche entscheidet, eine Verletzung des Schutzes personenbezogener nicht an die Aufsichtsbehörde zu melden, muss er nachweisen können, dass diese Verletzung nicht zu einem Risiko für den Betroffenen führt.

PFLICHT ZUR BENACHRICHTIGUNG DER BETROFFENEN PERSON:

- Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten der betroffenen Person zur Folge (Beispiele siehe oben), so besteht die **Pflicht**, die betroffene Person davon zu unterrichten.
- Der Verantwortliche hat die betroffene Person unverzüglich und in enger Zusammenarbeit mit der zuständigen Behörde und dem DSB zu **benachrichtigen** (siehe Artikel 34 Absatz 2).
- Unter bestimmten Umständen hat der Verantwortliche in Zusammenarbeit mit dem DSB sofortige Maßnahmen zu ergreifen,
  → z.B. wenn Kreditkartendaten oder andere sensible Informationen wie Passwörter für E-Mail-Konten betroffen sind.
- Die Benachrichtigung hat in „klarer und einfacher Sprache“ zu erfolgen. Die Benachrichtigung hat mindestens auf der Firmenwebsite und je nach Art der Verletzung zusätzlich über andere Kanäle zu erfolgen,
  → z.B. per E-Mail, Brief, Hotline

BENACHRICHTIGUNG VON GROUP PRIVACY:

- GPR ist in den folgenden Fällen gemäß § 30 BCRP vom DSB zu benachrichtigen:
  - Vorfälle mit möglicher Öffentlichkeitswirkung
  - Vorfälle mit Relevanz für mehr als ein Unternehmen
  - Vorfälle mit einem möglichen Schaden von über 500.000 EUR

Ferner ist GPR aufgrund der DSGVO zu benachrichtigen, wenn die lokale bzw. federführende Behörde in Deutschland angesiedelt ist (Einzelheiten können dem „Prozessmodell Incident Management“, IV.33.6, entnommen werden).

DOKUMENTATION:

- Das Unternehmen, mit dem sich die Aufsichtsbehörde im Zusammenhang mit dem Vorfall in Verbindung setzt, hat den Vorfall zu dokumentieren; der Auftragsverarbeiter unterstützt den Verantwortlichen (Artikel 28 und 29) hierbei. Zudem werden alle Vorfälle, über die GPR benachrichtigt wurde, auch von GPR dokumentiert.
- Das Prozessmodell für das Incidentmanagement und die Vorlage zur Meldung bei Datenschutzverletzungen sind von dem Unternehmen in seiner Eigenschaft als Verantwortlicher bzw. Auftragsverarbeiter zu verwenden, damit der Pflicht des Verantwortlichen entsprochen werden kann, jeden einzelnen Vorfall einschließlich "aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen" zu dokumentieren (Artikel 33 Absatz 5).

ERWÄGUNGEN IM FALLE EINER DATENSCHUTZVERLETZUNG NACH DER EPRIVACY-RICHTLINIE:

- Handelt es sich bei der Datenschutzverletzung um eine Verletzung der Sicherheit von Daten im Bereich der elektronischen Kommunikation, hat das nationale Gesetze zur Umsetzung der ePD Vorrang. Die Anforderungen an die Benachrichtigung des Bereichs GPR bleiben weiterhin gültig (§ 30 BCRP).

IV.33, 34.4 Fragebogen zur Compliance

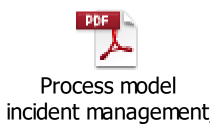
- Gibt es in Ihrem Unternehmen ein Prozess für das Incidentmanagement? [Ja]/[Nein]
- Werden in Ihrem Unternehmen etwaige Datenschutzverletzungen gemäß den Anforderungen der DSGVO dokumentiert? [Ja]/[Nein]
- Gibt es in Ihrem Unternehmen ein Verfahren für die Meldung von Datenschutzverletzungen ? [Ja]/[Nein]

IV.33, 34.5 Sanktionen

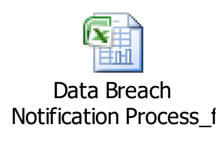
- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

IV.33, 34.6 Best Practices und Vorlagen

- Prozessmodell für das Incidentmanagement



- Verfahren für die Meldung von Datenschutzverletzungen (englische Version):



ARTIKEL 35 DATENSCHUTZ-FOLGENABSCHÄTZUNG

ARTIKEL 36 VORHERIGE KONSULTATION

IV. 35, 36.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 35 Datenschutz-Folgenabschätzung (Kapitel IV – Verantwortlicher und Auftragsverarbeiter) Artikel 36 Vorherige Konsultation (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	84, 89 bis 96
Querverweise	Artikel 39 Absatz 1 Buchstabe c
Zugehörige Unterlagen	Leitfaden für die Durchführung einer Datenschutz-Folgenabschätzung, herausgegeben vom British Information Commissioner's Office
BCRP Verweise	§ 11 Automatisierte Einzelentscheidungen § 13 Besondere Arten personenbezogener Daten § 31 Überprüfungen des Datenschutzniveaus § 33 Zusammenarbeit mit Aufsichtsbehörden

IV. 35, 36.2 Zusammenfassung

Artikel 35 verpflichtet Verantwortliche dazu, in bestimmten Verarbeitungssituationen Datenschutz-Folgenabschätzungen (DSFA) vorzunehmen, und beschreibt die diesbezüglichen Anforderungen. Die DSFA soll Risiken für Verstöße ermitteln und miniimieren.

Nach Artikel 36 ist der Verantwortliche verpflichtet, die Aufsichtsbehörde vor der Verarbeitung zu konsultieren, wenn aus einer DSFA ein hohes unabwendbares Risiko hervorgeht.

IV. 35, 36.3 Binding Interpretations

DATENSCHUTZ-FOLGENABSCHÄTZUNG

- Umsetzung des PSA-Verfahrens: Damit die Einhaltung der gesetzlichen Vorgaben der DSGVO sowie sämtlicher darin festgelegter Datenschutz- und Sicherheitsanforderungen jederzeit gewährleistet ist,

ist das PSA-Verfahren in der gültigen, von GPR bereitgestellten Fassung in jedem zum Konzern Deutsche Telekom zugehörigen Unternehmen umzusetzen.

WEITERE EINZELHEITEN:

- DSB: Der Rat des bestellten DSB ist einzuholen. Das PSA-Verfahren gewährleistet, dass sämtliche Prozesse/Systeme der Kategorie A vom zuständigen Datenschutzbereich beurteilt werden.
- Risikobewertung: Die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge und der damit verbundenen Risiken ist Teil der Erstberatung, welche auch Maßnahmen des PSA-Verfahrens beinhaltet. Aus diesem Grund haben sämtliche Unternehmen des Konzerns Deutsche Telekom den „Initial Consultation Guide“ von GPR zu beachten.
- Relevante Verarbeitung: Zukünftig wird die Aufsichtsbehörde „schwarze“ und „weiße“ Listen bereitstellen (siehe Artikel 35 Absatz 4 und 5), aus denen die Verarbeitungstätigkeiten hervorgehen, die mindestens bei der Datenschutz-Folgenabschätzung zu betrachten sind. Insoweit erforderliche Anpassungen werden im PSA-Portal in Form von Änderungsmitteilungen angezeigt, die zweimal im Jahr vom Security Demand Management (SDM) herausgegeben werden.
- Genehmigte Verhaltensregeln: Genehmigte Verhaltensregeln werden in Form von zentralen Datenschutzanforderungen umgesetzt. Sämtliche Unternehmen des Konzerns Deutsche Telekom haben diese Anforderungen einzuhalten.

VORHERIGE KONSULTATION:

- Konsultation der Aufsichtsbehörde und Einbeziehung des DSB: Falls die Datenverarbeitung mit einem hohen Risiko verbunden ist und keine Maßnahmen zur Eindämmung des Risikos getroffen werden, hat der Verantwortliche die Aufsichtsbehörde vor der Verarbeitung zu konsultieren. Der Verantwortliche hat den DSB seines Unternehmens im Vorfeld gemäß § 28 Absatz 7 BCRP einzubeziehen.
- Einbeziehung des Konzerndatenschutzbeauftragten: Der Konzerndatenschutzbeauftragte ist – zusätzlich – zu konsultieren, wenn die Datenverarbeitung mehr als ein Konzernunternehmen betrifft oder mit einem Schaden von über 500.000 EUR zu rechnen ist. Der Konzerndatenschutzbeauftragte ist darüber hinaus zu informieren, wenn sich die für ein Unternehmen geltenden Gesetze wesentlich nachteilig im Sinne der BCRP ändern (siehe § 30 BCRP).

IV. 35, 36.4 Fragebogen zur Compliance

- Wurde das PSA-Verfahren in der gültigen, von GPR bereitgestellten Fassung umgesetzt? [Ja]/[Nein]
- Ist das PSA-Verfahren mit allen relevanten Elementen in Ihrer Organisation verpflichtend? [Ja]/[Nein]
- Besteht ein enger Zusammenhang zwischen den Produktentwicklungsprozessen und dem eingeführten PSA-Verfahren, durch den sichergestellt ist, dass jedes neue System bzw. Produkt das PSA-Verfahren durchläuft? [Ja]/[Nein]

IV. 35, 36.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

IV.35, 36.6 Best Practices und Vorlagen

- PSA: https://drc.telekom.de/de/sec/privacy-security-assessment

ARTIKEL 37 BENENNUNG EINES DATENSCHUTZBEAUFTRAGTEN

IV.37.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 37 – Benennung eines Datenschutzbeauftragten (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	97
Querverweise	Keine
Zugehörige Unterlagen	Arbeitspapier 236: Erklärung zum Maßnahmenplan 2016 für die Umsetzung der Datenschutz-Grundverordnung (DSGVO)
BCRP Verweise	§ 28 Datenschutzbeauftragter § 29 Konzerndatenschutzbeauftragter

37.2 Zusammenfassung

Dieser Artikel regelt, wann vom Verantwortlichen bzw. vom Auftragsverarbeiter ein Datenschutzbeauftragter (DSB) zu benennen ist, und legt unterschiedliche Optionen für eine solche Benennung fest.

37.3 Binding Interpretations

KONZERNDATENSCHUTZBEAUFTRAGTER UND LOKALER DATENSCHUTZBEAUFTRAGTER:

- Der Konzern Deutsche Telekom hat den Leiter des Bereichs GPR zum Konzerndatenschutzbeauftragten bestellt. Jedes zum Konzern Deutsche Telekom zugehörige Unternehmen hat einen unabhängigen DSB zu benennen. Bereits bestellte DSB bleiben im Amt.
- Der Konzerndatenschutzbeauftragte ist per E-Mail unter datenschutz@telekom.de/privacy@telekom.de und telefonisch unter +49 228 181 82001 zu erreichen (siehe Artikel 37 Absatz 2 und § 29 BCRP). Die Kontaktdaten des Konzerndatenschutzbeauftragten und der DSB der Unternehmen werden von den Unternehmen nach innen und nach außen kommuniziert und der Aufsichtsbehörde mitgeteilt (siehe Artikel 37 Absatz 1 und 7, § 28 BCRP).

FÄHIGKEITEN UND BERUFLICHE QUALIFIKATION:

- Das Internationale Governance-Modell von Group Privacy, Deutsche Telekom AG (Modul 1.1 Kompetenzprofil des Datenschutzbeauftragten, Modul 2.1 Verantwortlichkeiten des

Unternehmens/Vorstands) und § 28 BCRP enthalten Einzelheiten zu den Kompetenzen und Fähigkeiten von Datenschutzbeauftragten im Konzern Deutsche Telekom (siehe Artikel 37 Absatz 5).

37.4 Fragebogen zur Compliance

- Wurde ein Konzerndatenschutzbeauftragter benannt? [Ja]/[Nein]
- Wurde vom Unternehmen ein DSB bestellt? [Ja]/[Nein]
- Wurden die Kontaktdaten des Konzerndatenschutzbeauftragten und des DSB veröffentlicht und der Aufsichtsbehörde mitgeteilt? [Ja]/[Nein]
- Erfüllt der DSB die Qualifikationsanforderungen des Konzerns Deutsche Telekom? [Ja]/[Nein]

37.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

37.6 Best Practices und Vorlagen

- Internationales Governance-Modell (englische Version):



ARTIKEL 38 STELLUNG DES DATENSCHUTZBEAUFTRAGTEN

IV.38.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 38 – Stellung des Datenschutzbeauftragten (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	Keine
Querverweise	Artikel 37; 39
Zugehörige Unterlagen	Arbeitspapier 236: Erklärung zum Maßnahmenplan 2016 für die Umsetzung der Datenschutz-Grundverordnung (DSGVO)
BCRP Verweise	§ 28 Datenschutzbeauftragter § 29 Konzerndatenschutzbeauftragter

IV.38.2 Zusammenfassung

In diesem Artikel sind die Rechte und die Stellung des DSB innerhalb der Organisation des Verantwortlichen und des Auftragsverarbeiters festgelegt.

IV.38.3 Binding Interpretations

STELLUNG UND BETEILIGUNG DES DATENSCHUTZBEAUFTRAGTEN:

- Die Bestimmungen in § 28 und § 24 BCRP und im Internationalen Governance-Modell von Group Privacy, Deutsche Telekom AG erfüllen die Anforderungen der DSGVO:
  - → Beispielsweise Unabhängigkeit des DSB: Ausstattung mit den erforderlichen finanziellen und personellen Mitteln, Berichtsrecht, organisatorische Anbindung an die Unternehmensleitung, frühzeitige Beteiligung bei jeglichen Datenschutzbelangen und Recht der betroffenen Person, sich an den DSB zu wenden
- Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden (siehe Artikel 38 Absatz 3).

IV.38.4 Fragebogen zur Compliance

- Verfügt der DSB über angemessene finanzielle und personelle Mittel, um nationale und konzernweite Datenschutzanforderungen umzusetzen? [Ja]/[Nein]

(Der DSB sollte in der Lage sein, die Geschäftsbereiche in Datenschutzbelangen zu unterstützen und die Einhaltung der Datenschutzbestimmungen innerhalb des Unternehmens sicherzustellen.)

- Berichtet der DSB direkt an die Unternehmensleitung? [Ja]/[Nein]
- Bestehen angemessene Prozesse und Abläufe, um sicherzustellen, dass der DSB angemessen und frühzeitig bei allen Angelegenheiten, die den Schutz personenbezogener Daten betreffen, beteiligt wird? (z.B. PSA) [Ja]/[Nein]
- Gibt es eine einfache Möglichkeit, sich mit dem DSB in Verbindung zu setzen (z.B. im Intranet/Internet veröffentlichte Kontaktdaten)? [Ja]/[Nein]
- Nimmt der DSB neben seiner Tätigkeit als DSB andere Aufgaben wahr? Falls ja, führen derartige Aufgaben zu einem Interessenkonflikt? [Ja]/[Nein]

IV.38.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

IV.38.6 Best Practices und Vorlagen

- E-Mail-Funktionspostfächer der DSB für das lokale Beschwerdeverfahren, z.B privacy@telekom.de.
- Internationales Governance-Modell (englische Version):



ARTIKEL 39 AUFGABEN DES DATENSCHUTZBEAUFTRAGTEN

IV.39.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 39 – Aufgaben des Datenschutzbeauftragten (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	Keine
Querverweise	Artikel 37; 38
Zugehörige Unterlagen	Arbeitspapier 236: Erklärung zum Maßnahmenplan 2016 für die Umsetzung der Datenschutz-Grundverordnung (DSGVO)
BCRP Verweise	§ 28 Datenschutzbeauftragter § 29 Konzerndatenschutzbeauftragter

IV.39.2 Zusammenfassung

Dieser Artikel regelt die Aufgaben und Pflichten des DSB.

IV.39.3 Binding Interpretations

ALLGEMEINE AUFGABEN DES DSB:

- Siehe §§ 27, 28, 31, 32 und 33 BCRP:

  → Beispielsweise Informations- und Beratungspflicht in Datenschutzbelangen und in Bezug auf die Datenschutz-Folgenabschätzung, Überwachung, Schulung und Zusammenarbeit mit der Aufsichtsbehörde

  → Zudem erfüllt das Internationale Governance-Modell von Group Privacy, Deutsche Telekom AG (siehe IV.39.6) zusammen mit dem PSA-Verfahren (siehe IV.35, 36.6) die Anforderungen an das Aufgabenprofil des DSB.

ÜBERWACHUNG DER EINHALTUNG VON DATENSCHUTZVORSCHRIFTEN:

- Jeder DSB hat die Einhaltung der DSGVO und anderer gesetzlicher Bestimmungen bzw. interner Unternehmens-/Konzernvorgaben für den Datenschutz zu überwachen (siehe Artikel 39 Absatz 1 Buchstabe b und § 28 Absatz 1 BCRP). Die Überwachungspflicht ist in § 31 BCRP konkretisiert.

- Die abschließende Verantwortung für die Einhaltung der DSGVO und die entsprechende Rechenschaftspflicht liegt bei der Unternehmensführung, nicht beim DSB (siehe Artikel 5 Absatz 2).

IV.39.4 Fragebogen zur Compliance

- Verfügen Sie über ein Schulungskonzept? [Ja]/[Nein]
- Wurde das internationale PSA-Verfahren in die Produkt- und Systementwicklungsprozesse integriert? [Ja]/[Nein]
- Entscheiden Sie sich für eine der Alternativen:
  - → Keine PSA-Umsetzung
  - → Nur die wesentlichen Anforderungen des PSA-Verfahrens wurden umgesetzt.
  - → Das PSA-Verfahren wurde vollumfänglich umgesetzt (Nutzung des PSA-Portals – ungeänderte Fassung).
- Gibt es ein Konzept zur Überwachung der Einhaltung der DSGVO? [Ja]/[Nein]
- Wird die Einhaltung der DSGVO, anderer gesetzlicher Bestimmungen und interner Unternehmens-/Konzernvorgaben für den Datenschutz in Ihrem Unternehmen regelmäßig geprüft? [Ja]/[Nein]
- Werden die regelmäßigen Überprüfungen dokumentiert und wird die Unternehmensleitung über das Ergebnis der Prüfungen informiert? [Ja]/[Nein]

39.5 Sanktionen

- Artikel 83 Absatz 4 Buchstabe a: 10.000.000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes.

39.6 Best Practices und Vorlagen

- Internationales Governance-Modell von Group Privacy, Deutsche Telekom AG (englische Version):



- Kommunikations- und Risikokonzept:



- Nationale Konzernrichtlinie zur Organisation des Datenschutzes/Wahrnehmung der Verantwortung für die Datenverarbeitung:



ARTIKEL 42 ZERTIFIZIERUNG

ARTIKEL 43 ZERTIFIZIERUNGSSTELLEN

IV.42, 43.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 42 Zertifizierung (Kapitel IV – Verantwortlicher und Auftragsverarbeiter)
DSGVO ErwGr	100
Querverweise	Artikel 24 Absatz 3; Artikel 25 Absatz 3; Artikel 28 Absatz 5 und 6; Artikel 32 Absatz 3; Artikel 46 Absatz 2 Buchstabe f, Artikel 83 Absatz 4 Buchstabe b
Zugehörige Unterlagen	Keine
BCRP Verweise	Keine

IV.42, 43.2 Zusammenfassung

Artikel 42 legt die Rahmenbedingungen für eine Datenschutzzertifizierung fest. Der Verantwortliche und der Auftragsverarbeiter können auf dieser Grundlage durch genehmigte Zertifizierungsmechanismen sowie Datenschutzsiegel und -prüfzeichen nachweisen, dass die DSGVO eingehalten wird.

Die geltenden Anforderungen hinsichtlich Zertifizierungsstellen sind in Artikel 43 beschrieben.

Das neue Konzept der Zertifizierung von Datenschutzmechanismen (vgl. Überblick über die Zertifizierung gemäß IV.42, 43.6) kann dazu beitragen, einen verlässlichen und prüfbaren Rahmen für den Datenschutz zu schaffen. Dieser Rahmen wird von den Aufsichtsbehörden und der Europäischen Kommission erarbeitet.

IV.42, 43.3 Best Practices und Vorlagen

- Überblick über die Zertifizierung



Zertifizierung.pdf

KAPITEL V – ÜBERMITTLUNGEN PERSONENBEZOGENER DATEN AN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

Artikel 44 bis 50

In diesem Kapitel wird die Übermittlung personenbezogener Daten in Drittländer oder internationale Organisationen behandelt. Zudem werden die einzelnen Instrumente aufgeführt, die im Rahmen einer solchen grenzüberschreitenden Übermittlung als Rechtsgrundlage dienen können. Zu diesen Instrumenten gehören die Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses, die Datenübermittlung vorbehaltlich geeigneter Garantien und verbindliche interne Datenschutzvorschriften. Ferner wird in diesem Kapitel die Datenübermittlung auf der Grundlage gerichtlicher Urteile oder von Entscheidungen der Verwaltungsbehörden von Drittländern behandelt.

ARTIKEL 44 ALLGEMEINE GRUNDSÄTZE DER DATENÜBERMITTLUNG

ARTIKEL 45 DATENÜBERMITTLUNG AUF DER GRUNDLAGE EINES ANGEMESSENHEITSBESCHLUSSES

ARTIKEL 46 DATENÜBERMITTLUNG VORBEHALTLICH GEEIGNETER GARANTIEN

ARTIKEL 48 NACH DEM UNIONSRECHT NICHT ZULÄSSIGE ÜBERMITTLUNG ODER OFFENLEGUNG

ARTIKEL 49 AUSNAHMEN FÜR BESTIMMTE FÄLLE

V.44–46, 48–49.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 44 – Allgemeine Grundsätze der Datenübermittlung (Kapitel V – Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) Artikel 45 – Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses (Kapitel V – Übermittlungen

	personenbezogener Daten an Drittländer oder an internationale Organisationen) Artikel 46 – Datenübermittlung vorbehaltlich geeigneter Garantien (Kapitel V – Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) Artikel 48 – Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung (Kapitel V – Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) Artikel 49 – Ausnahmen für bestimmte Fälle (Kapitel V – Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen)
DSGVO ErwGr	101 bis 109, 111 bis 115
Querverweise	Artikel 4; 6; 40; 42; 47
Zugehörige Unterlagen	Keine
BCRP Verweise	§ 17 Übermittlung von Daten

V.44–46, 48–49.2 Zusammenfassung

In den Artikeln 44 bis 49 der DSGVO sind die Bedingungen für die internationale Übermittlung von Daten in Drittländer geregelt.

Die Drittländer (außerhalb der EU und des EWR[2]) müssen ein angemessenes Datenschutzniveau gewährleisten.

Die DSGVO enthält verschiedene Möglichkeiten, wie ein angemessenes Datenschutzniveau erreicht und bewertet werden kann:

1. Angemessenheitsbeschluss der Kommission: Die Europäische Kommission kann beschließen, dass ein Drittland, ein Gebiet, ein Sektor oder internationale Organisationen ein angemessenes Schutzniveau bieten (Artikel 45).
2. Geeignete Garantien: Daten dürfen in ein Drittland übermittelt werden, wenn geeignete Garantien vorliegen, z.B. verbindliche interne Datenschutzvorschriften, Standard-Datenschutzklauseln und genehmigte Zertifizierungsmechanismen. (Artikel 46)

[2] Europäischer Wirtschaftsraum

3. Die Datenübermittlung in ein Drittland aufgrund eines Gerichtsurteils oder einer Entscheidung von Verwaltungsbehörden ist nur dann zulässig, wenn sie sich auf eine internationale Übereinkunft stützt (Artikel 48).
4. Ausnahmen: Falls weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen, ist eine Übermittlung in ein Drittland nur zulässig, wenn bestimmte Bedingungen erfüllt werden, beispielsweise die betroffene Person in die Übermittlung ausdrücklich eingewilligt hat (Artikel 49).

V.44–46, 48–49.3 Binding Interpretations

ÜBERMITTLUNG VON DATEN IN EIN DRITTLAND:

- **Genehmigung:** Die Übermittlung von Daten in ein Drittland, einschließlich des von einem Drittland ausgehenden Zugriffs auf die Daten, ist zulässig, wenn die Datenverarbeitung an sich rechtmäßig ist und das Drittland, in dem der Empfänger der Daten niedergelassen ist, ein angemessenes Schutzniveau bietet (siehe Artikel 44 bis 49). Diese Bestimmungen gelten auch für die Weiterübermittlung der Daten innerhalb des Drittlands oder in ein anderes Drittland und unabhängig davon, ob die Übermittlung zwischen zwei Verantwortlichen oder zwischen einem Verantwortlichen und einem Auftragsverarbeiter erfolgt. Die Rechtmäßigkeit der Datenverarbeitng bedeutet, dass im Falle einer Auftragsverarbeitung, zusätzlich zu einem angemessenen Datenschutzniveau, eine Datenverarbeitungsvereinbarung notwendig ist.
- **Verantwortung:** Unabhängig davon, ob der Auftragsverarbeiter in der EU/im EWR ansässig ist oder nicht, sind der Verantwortliche und der Auftragsverarbeiter für die rechtmäßige Datenübermittlung verantwortlich.

GARANTIEN:

- Bei der Auswahl der geeigneten Garantien für die Übermittlung von Daten in ein Drittland sollte folgendermaßen vorgegangen werden:
  - → Datenübermittlung von einem Unternehmen des Konzerns Deutsche Telekom an ein Unternehmen des Konzerns Deutsche Telekom in einem Drittland: Die BCRP wurden von dem datenübermittelnden Konzernunternehmen und von dem datenempfangenden Konzernunternehmen unterzeichnet und dienen als angemessene Garantie. Gleiches gilt für die Weiterübermittlung an ein weiteres Konzernunternehmen in einem Drittland.
  - → Datenübermittlung an externe Unternehmen in Drittländern: Die von der Kommission verabschiedeten Standarddatenschutzklauseln sind zu unterzeichnen.
  - → Besondere Fälle: Es ist eine Abstimmung mit dem Bereich GPR bzw. dem zuständigen DSB erforderlich. Grundsätzlich dürfen die unter Artikel 49 Absatz 1 Satz 2 aufgeführten Ausnahmen nicht verwendet werden.

V.44–46, 48-49.4 Fragebogen zur Compliance

- Übermitteln Sie personenbezogene Daten in Drittländer bzw. erlauben Sie ein Zugriff aus Drittländern auf personenbezogene Daten? [Ja]/[Nein]
- Falls ja, wurde geprüft, ob ein entsprechender Angemessenheitsbeschluss vorliegt? [Ja]/[Nein]

- Sollte kein solcher Beschluss vorliegen, wurde sichergestellt, dass die entsprechenden Garantien (z.B. BCRP, EU-Standardvertragsklauseln) bestehen? [Ja]/[Nein]
- Werden die Anforderungen an die Transparenz (z.B. Artikel 13 Absatz 1 Buchstabe f und Artikel 14 Absatz 1 Buchstabe f) und Dokumentation (Artikel 30) erfüllt? [Ja]/[Nein]
- Im Falle einer Auftragsverarbeitung, ist eine Datenverarbeitungsvereinbarung vorhanden? [Ja]/[Nein]

V.44–46,48-49.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe c: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes.

V.44–46,48–49.6 Best Practices und Vorlagen

Keine

ARTIKEL 47 VERBINDLICHE INTERNE DATENSCHUTZVORSCHRIFTEN

V.47.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 47 – Verbindliche interne Datenschutzvorschriften (Kapitel V – Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen)
DSGVO ErwGr	110
Querverweise	Artikel 13; 14; 22; 37; 49; 63; Artikel 70 Absatz 1 Buchstabe c und i; Artikel 79
Zugehörige Unterlagen	Arbeitspapier 74: Arbeitsdokument: Übermittlung personenbezogener Daten an Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche interne Datenschutzvorschriften für die internationale Datenübermittlung; Arbeitspapier 133: Empfehlung 1/2007 für den Standardantrag auf die Genehmigung verbindlicher interner Datenschutzvorschriften für die Übermittlung personenbezogener Daten; Arbeitspapier 153: Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher interner Datenschutzvorschriften; Arbeitspapier 154: Arbeitsdokument „Rahmen für verbindliche interne Datenschutzvorschriften“; Arbeitspapier 155, Version 04: Arbeitsdokument zu „Häufig gestellten Fragen“ über verbindliche interne Datenschutzvorschriften
BCRP Verweise	Richtlinie zum Schutz der Persönlichkeitsrechte im Umgang mit personenbezogenen Daten in der Deutschen Telekom Gruppe Version 2.7, Stand 5. Dezember 2013, Status: *finale Fassung*

V.47.2 Zusammenfassung

In Artikel 47 werden die an verbindliche interne Datenschutzvorschriften gestellten Anforderungen ausführlich behandelt. Gemäß Artikel 46 Absatz 5 bleiben Genehmigungen, die von einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilt wurden, so lange gültig, bis sie von dieser

Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden. Wesentliche Änderungen der BCRP sind mit der Aufsichtsbehörde abzustimmen.

V.47.3 Binding Interpretations

GÜLTIGKEIT DER BESTEHENDEN BCRP:

- Die „Konzernrichtlinie Datenschutz – Binding Corporate Rules Privacy (BCRP) – Richtlinie zum Schutz der Persönlichkeitsrechte im Umgang mit personenbezogenen Daten in der Deutschen Telekom Gruppe" (Version 2.7, Stand 5. Dezember 2013, Status: finale Fassung) bleibt gültig.
- Die bestehenden BCRP werden um die Binding Interpretations zur DSGVO ergänzt.

V.47.4 Fragebogen zur Compliance

- Steht Ihre lokale Datenschutzorganisation vollständig im Einklang mit Teil 4 „Datenschutzorganisation" der BCRP? [Ja]/[Nein]
- Besteht in Ihrem Unternehmen ein Meldeverfahren zur Unterrichtung der Aufsichtsbehörde über etwaige rechtliche Bestimmungen in Ihrem Land, die die Garantien der BCRP beeinträchtigen könnten (Artikel 47 Absatz 2 Buchstabe m sowie § 33 BCRP)? [Ja]/[Nein]
- Bietet Ihr Unternehmen geeignete Datenschutzschulungen für Beschäftigte mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten an (Artikel 47 Absatz 2 Buchstabe b) sowie § 32 BCRP)? [Ja]/[Nein]
- Nimmt Ihr Unternehmen alle im Internationalen Governance-Modell von Group Privacy, Deutsche Telekom AG aufgeführten Aufgaben wahr? [Ja]/[Nein]
- Informiert Ihr Unternehmen die Aufsichtsbehörde und die betroffene Person über Struktur und Kontaktdaten des Konzerns und seiner Unternehmen (Artikel 47 Absatz 2 Buchstabe a sowie § 42 BCRP)? [Ja]/[Nein]
- Bestehen Verfahren für die Erfassung von Änderungen der BCRP und ihre Meldung an die Aufsichtsbehörde (Artikel 47 Absatz 2 Buchstabe k)? [Ja]/[Nein]
- Werden die Maßnahmen und Verfahren, auf die in Artikel 47 Absatz 2 Buchstabe l und j verwiesen wird, dokumentiert (Artikel 47 Absatz 2 Buchstabe l und j sowie § 31 Absatz 2 BCRP)? [Ja]/[Nein]

V.47.5 Sanktionen

- Artikel 83 Absatz 5 Buchstabe c: 20.000.000 EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes.

V.47.6 Best Practices und Vorlagen

- Internationales Governance-Modell von Group Privacy, Deutsche Telekom AG (englische Version):



- Vorlage zur vierteljährlichen Berichterstattung, GPR International (englische Version):


Quartely reporting
template.pdf

KAPITEL VIII – RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

Artikel 77 bis 84

In diesem Kapitel werden die Rechtsbehelfe behandelt, die einer betroffenen Person bei einer vermuteten Verletzung der DSGVO bei der Verarbeitung ihrer personenbezogenen Daten zustehen: Recht auf Beschwerde bei einer Aufsichtsbehörde, Recht auf wirksamen gerichtlichen Rechtsbehelf und Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Bei Verstößen gegen die DSGVO können Aufsichtsbehörden wirksame, verhältnismäßige und abschreckende Sanktionen und Geldbußen verhängen. Die Bußgeldsätze für Verstöße wurden gegenüber früheren Regelungen erheblich angehoben. Es wurden zwei Bußgeldsätze festgelegt:

- Geldbußen von bis zu 10.000.000 EUR oder bei Unternehmen bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs
- Geldbußen von bis zu 20.000.000 EUR oder bei Unternehmen bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Aus dem Kapitel geht eindeutig hervor, welcher Bußgeldsatz für welche Verstöße zutrifft.

Die Mitgliedstaaten können Vorschriften über weitere Sanktionen insbesondere für Verstöße festlegen, die keiner Geldbuße gemäß Artikel 83 unterliegen.

ARTIKEL 82 HAFTUNG UND RECHT AUF SCHADENERSATZ

VIII.82.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 82 – Haftung und Recht auf Schadenersatz
DSGVO ErwGr	146, 147
Querverweise	Artikel 26; 28; Artikel 47 Absatz 2 Buchstabe e; Artikel 62 Absatz 5; Artikel 80
Zugehörige Unterlagen	Keine
BCRP Verweise	Keine

VIII.82.2 Zusammenfassung

Artikel 82 regelt den Anspruch einer betroffenen Person auf Schadenersatz gegen den Verantwortlichen und den Auftragsverarbeiter im Falle eines Verstoßes gegen die DSGVO, aus der ihr ein materieller oder immaterieller Schaden entstanden ist. In Artikel 82 wird zudem geklärt, in welchem Verhältnis die Haftung zwischen Verantwortlichen und Auftragsverarbeitern aufgeteilt wird. Um eine Haftung zu vermeiden, hat der Verantwortliche bzw. der Auftragsverarbeiter nachzuweisen, dass er nicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Der Artikel enthält Regelungen für den Fall, dass mehr als ein Verantwortlicher bzw. Auftragsverarbeiter oder sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter beteiligt sind.

VIII.82.3 Binding Interpretations

ALLGEMEIN:

- Gemäß DSGVO haftet der Auftragsverarbeiter entweder unabhängig oder gesamtschuldnerisch gegenüber der betroffenen Person. Aus diesem Grund ist zu gewährleisten, dass die vertraglichen Verpflichtungen und die Verpflichtungen nach DSGVO erfüllt werden und dies hinreichend dokumentiert wird. Der Nachweis über die ordnungsgemäße Erfüllung dieser Verpflichtungen ist Voraussetzung für eine Haftungsbefreiung (siehe Artikel 82 Absatz 3).

GESAMTSCHULDNERISCHE HAFTUNG:

- **Zur Minderung des Haftungsrisikos** in Form einer gesamtschuldnerischen Haftung ist eine klare Beschreibung der gegenseitigen Verpflichtungen und die Dokumentation der Weisungen des Verantwortlichen von entscheidender Bedeutung. Nach der DSGVO hat der Auftragsverarbeiter die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen, schriftlich oder elektronisch, z.B. E-Mail, (siehe Artikel 28 Absatz 3 Buchstabe a und Artikel 29) zu verarbeiten. Dieser Grundsatz gilt entsprechend für Unterauftragsverarbeiter des Auftragsverarbeiters.
- **Zur Begrenzung des verbleibenden Haftungsrisikos** – falls das betreffende Unternehmen der Deutschen Telekom als gemeinsam Verantwortlicher (Artikel 82 Absatz 4) angesehen wird – ist die Liquidität des möglichen Vertragspartners im Vorfeld zu beurteilen. Sofern nicht schon vorhanden, müssen dafür geeignete Verfahren eingeführt werden.
- **Zurückforderung eines Teils des Schadenersatzes:** Falls ein Teil des von der betroffenen Person geltend gemachten Schadens von einem Unternehmen des Konzerns Deutsche Telekom verursacht worden ist und dieses Unternehmen für den gesamten Schaden haftbar gemacht wird, muss sichergestellt werden, dass es den Teil des Schadenersatzes zurückfordert, der dem Anteil der übrigen beteiligten Unternehmen an der Verantwortung für den Schaden entspricht (siehe Artikel 82 Absatz 4 und 5).
- **Vertragsklauseln bedürfen insoweit einer Überprüfung**, um sicherzustellen, dass sie keine Bestimmungen enthalten, wonach Vertragspartner Schadenersatzansprüche usw. ausschließen können.

VIII.82.4 Fragebogen zur Compliance

- Wird eine interne Risikobewertung durchgeführt? [Ja]/[Nein]
- Wird von der DTAG bzw. einem Unternehmen des Konzerns Deutsche Telekom geprüft, ob eine Dienstleistung, ein Produkt oder andere Einflussfaktoren (z.B. Partner, Unterauftragsverarbeiter oder ein Unternehmen als gemeinsam Verantwortlicher) unter Berücksichtigung eines möglichen Haftungsfalls, Schadenersatzanspruchs und eines nicht quantifizierbaren Schadenshöhe akzeptabel oder inakzeptabel sind? [Ja]/[Nein]
- Werden die internen Genehmigungsverfahren des Unternehmens geprüft? [Ja]/[Nein]
- Wird das mögliche Risiko für eine gesamtschuldnerische Haftung für beliebige Schäden (unter Berücksichtigung der Haftungsquote des Unterauftragnehmers oder Partners – auch „gemeinsam Verantwortlicher") bewertet? [Ja]/[Nein]
- Werden Vertragsklauseln zu Schadenersatzansprüchen und Haftung vereinbart? [Ja]/[Nein]
- Werden Schadenersatz und Haftung (soweit gesetzlich zulässig – gegenüber Vertragspartnern) eingeschränkt? [Ja]/[Nein]
- Verwenden Sie Klauseln, die dazu dienen, die Rückforderung von Schadenersatz von Vertragspartnern zu ermöglichen? [Ja]/[Nein]
- Prüfen Sie die Möglichkeit von Freistellungsklauseln für Fälle, in denen Sie Ihre Verantwortung für einen Umstand, durch den ein Schaden eingetreten ist, und Ihren Verantwortungsbereich klar abgrenzen können? [Ja]/[Nein]
- Haben Sie die Bewertung/Überprüfung der vertraglichen Leistung/des Produkts auf Konformität mit der DSGVO dokumentiert? [Ja]/[Nein]

VIII.82.5 Sanktionen

Keine

VIII.82.6 Best Practices und Vorlagen

Keine

ARTIKEL 83 ALLGEMEINE BEDINGUNGEN FÜR DIE VERHÄNGUNG VON GELDBUẞEN

VIII.83.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 83 – Allgemeine Bedingungen für die Verhängung von Geldbußen (Kapitel VIII – Rechtsbehelfe, Haftung und Sanktionen)
DSGVO ErwGr	148, 150 bis 151
Querverweise	Artikel 58; 78; 79; 82; 84,
Zugehörige Unterlagen	Keine
BCRP Verweise	§ 5 Informationspflicht § 22 Widerspruchsrecht und Recht auf Löschung, Sperrung und Berichtigung

VIII.83.2 Zusammenfassung

Die Aufsichtsbehörden sind berechtigt, zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Geldbußen in beträchtlicher Höhe zu verhängen. Je nach Art des Verstoßes können Geldbußen von bis zu 10.000.000 EUR bzw. 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (z.B. bei Verstößen gegen die Pflichten des Verantwortlichen und des Auftragsverarbeiters wie Datenschutz durch Technikgestaltung, Datenschutz-Folgenabschätzung und Führung von Verzeichnissen) oder von bis zu 20.000.000 EUR bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (z.B. bei Verstößen gegen die Bedingungen für die Einwilligung, die Rechte der betroffenen Person, die grenzüberschreitende Datenübermittlung oder bei Nichtbefolgung von Anweisungen von Aufsichtsbehörden) verhängt werden.

VIII.83.3 Binding Interpretations

FAKTOREN ZUR BESTIMMUNG DER BUSSGELDHÖHE:

- In jedem Einzelfall sind zur Minderung des Risikos von Geldbußen Maßnahmen zu ergreifen, um die Einhaltung der DSGVO sicherzustellen. Dazu zählen verbindliche interne Datenschutzvorschriften und geeignete Zertifizierungsmechanismen. Dies ist insoweit von Bedeutung, als die Aufsichtsbehörden diese Maßnahmen bei der Entscheidung über den Betrag der Geldbuße berücksichtigen (siehe Artikel 83 Absatz 2 DSGVO).

- Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden.
- Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag kann die Aufsichtsbehörde Folgendes berücksichtigen:
    - → Falls ein Verstoß gegen die DSGVO auf ein einzelnes Unternehmen des Konzerns und auf dessen eigene Betriebsumgebung zurückgeht, richtet sich der Betrag der Geldbuße nach dem Umsatz des betreffenden Unternehmens.
    - → Geht der Verstoß auf die Governance des Konzerns zurück, wird der Umsatz des Konzerns zur Bemessung der Geldbuße herangezogen.
- Neben den Geldbußen nach Artikel 83 besteht weiterhin die Möglichkeit von anderen Sanktionen einschließlich der persönlichen zivilrechtlichen und strafrechtlichen Verantwortung der Beschäftigten.

VIII.83.4 Fragebogen zur Compliance

- Wurde geprüft, wo sich genehmigte Zertifizierungsmechanismen in Ihrer Organisation vor dem Hintergrund der Verordnung und insbesondere von Artikel 83 DSGO als sinnvoll erweisen könnten? (Dies betrifft beispielsweise wichtige Prozesse mit den wichtigsten Daten.) Falls ja, sind weitere Zertifizierungen geplant? Sind die notwendigen Dokumentationen vorhanden? (Bewährtes Verfahren: SDSK des PSA-Verfahrens) [Ja]/[Nein]
- Wurden Ihre Risikoverzeichnisse in Anbetracht der erhöhten Geldbußen aktualisiert? [Ja]/[Nein]

VIII.83.5 Sanktionen

Keine

VIII.83.6 Best Practices und Vorlagen

- BCRP: https://drc.telekom.de/de/privacy/themen/binding-corporate-rules-privacy/39382

KAPITEL IX – VORSCHRIFTEN FÜR BESONDERE VERARBEITUNGSSITUATIONEN

Artikel 85 bis 91

Dieses Kapitel enthält Vorschriften für besondere Verarbeitungssituationen, beispielsweise die Datenverarbeitung im Beschäftigungskontext, die Verarbeitung und der Zugang der Öffentlichkeit zu amtlichen Dokumenten, die Verarbeitung zu im öffentlichen Interesse liegenden Archivierungszwecken und die Verarbeitung durch einen Verantwortlichen oder Auftragsverarbeiter, der Geheimhaltungspflichten unterliegt. Die DSGVO überlässt es den Mitgliedstaaten, eigene nationale Regelungen für die Verarbeitung in diesen Situationen zu treffen.

ARTIKEL 88 DATENVERARBEITUNG IM BESCHÄFTIGUNGSKONTEXT

IX.88.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 88 – Datenverarbeitung im Beschäftigungskontext (Kapitel IX – Vorschriften für besondere Verarbeitungssituationen)
DSGVO ErwGr	155
Querverweise	Artikel 4 Absatz 18 und 19
Zugehörige Unterlagen	Keine
BCRP Verweise	Keine

IX.88.2 Zusammenfassung

Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen (zum Beispiel Betriebsvereinbarungen) detailliertere Vorschriften und Verfahren für die Datenverarbeitung im Beschäftigungskontext festlegen.

IX.88.3 Binding Interpretations

BESTEHENDE KOLLEKTIVVEREINBARUNGEN UND BETRIEBSVEREINBARUNGEN:

- Diese sind bis Mai 2018 auf die DSGVO und das Recht des jeweiligen Mitgliedstaats abzustimmen.

ÜBERMITTLUNG VON MITARBEITERDATEN:

- Gemäß Artikel 88 Absatz 2 ist die Möglichkeit gegeben, in Kollektivvereinbarungen und Betriebsvereinbarungen Regelungen für die Übermittlung personenbezogener Daten innerhalb des Konzerns zu treffen.

IX.88.4 Fragebogen zur Compliance

- Stimmen die in Ihrem Unternehmen bestehenden Kollektivvereinbarungen und Betriebsvereinbarungen mit der DSGVO und dem Recht des jeweiligen Mitgliedstaats überein? [Ja]/[Nein]

IX.88.5 Sanktionen

Keine

IX.88.6 Best Practices und Vorlagen

Keine

KAPITEL XI – SCHLUSSBESTIMMUNGEN

Artikel 94 bis 99

Das letzte Kapitel enthält die Schlussbestimmungen, z.B. zur Aufhebung der Richtlinie 95/46/EG, zum Verhältnis der DSGVO zur ePD sowie zum Inkrafttreten und zur Anwendung.

ARTIKEL 94 AUFHEBUNG DER RICHTLINIE 95/46/EG

ARTIKEL 99 INKRAFTTRETEN UND ANWENDUNG

XI.94., 99.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 94 – Aufhebung der Richtlinie 95/46/EG (Kapitel XI – Schlussbestimmungen) Artikel 99 – Inkrafttreten und Anwendung (Kapitel XI – Schlussbestimmungen)
DSGVO ErwGr	171
Querverweise	Artikel 7
Zugehörige Unterlagen	Keine
BCRP Verweise	Keine

X.94, 99.2 Zusammenfassung

Die DSGVO ist am 24. Mai 2016 in Kraft getreten. Sie ist ab 25. Mai 2018 anzuwenden. Die Richtlinie 95/46/EG wird mit Wirkung vom 25. Mai 2018 aufgehoben.

X.94, 99.3 Binding Interpretations

UMSETZUNG DER DSGVO UND KONFORMITÄT:

- Während des zweijährigen Übergangszeitraums zwischen dem Inkrafttreten der DSGVO und ihrer Anwendung ist jeder Vorgang zur Verarbeitung personenbezogener Daten innerhalb des Konzerns Deutsche Telekom mit der DSGVO in Einklang zu bringen.
- Die Binding Interpretations zu den ausgewählten, im vorliegenden Dokument enthaltenen Artikeln der DSGVO sind zu beachten.

BESTEHENDE EINWILLIGUNG:

- Beruht die Verarbeitung personenbezogener Daten auf der Einwilligung der betroffenen Person, so ist es nicht erforderlich, diese Einwilligung nach dem Datum, ab dem die DSGVO anzuwenden ist, erneuern zu lassen, wenn die beiden folgenden Bedingungen erfüllt sind:
  - → Die bestehende Einwilligung wurde gemäß der Richtlinie 95/46/EG erteilt.
  - → Die Art und Weise, in der die bestehende Einwilligung erteilt wurde, entspricht den Bedingungen gemäß Artikel 6 Absatz 1 Buchstabe a, Artikel 7 und 8 sowie Artikel 9 Absatz 2 Buchstabe a der DSGVO.
- Aufgrund des verbindlichen Charakters der DSGVO gelten diese Anforderungen ausnahmslos konzernweit. Nationale Abweichungen sind nicht vorgesehen.
- Dasselbe gilt für Einwilligungen, die in Belangen erteilt wurden, die unter die ePrivacy-Richtlinie (ePD) fallen. Gemäß Artikel 2 Buchstabe f der ePD entspricht die Einwilligung eines Nutzers oder Teilnehmers der Einwilligung der betroffenen Person im Sinne der Richtlinie 95/46/EG, ohne dass zusätzliche Anforderungen an die Form der Einwilligung gestellt werden müssen (siehe Artikel 88).

ANWENDUNG DER DSGVOO:

- Die DSGVO darf vor dem 25. Mai 2018 weder vollständig noch teilweise angewandt werden.

X.94, 99.4 Fragebogen zur Compliance

- Entsprechen die vorhandenen Einwilligungen, die betroffene Personen Ihrem Unternehmen gegeben haben, der DSGVO? [Ja]/[Nein]
- Hat Ihr Unternehmen die hierin enthaltenen Binding Interpretations zu den Artikeln der DSGVO beachtet? [Ja]/[Nein]

X.94, 99.5 Sanktionen

Keine

X.94, 99.6 Best Practices und Vorlagen

Keine

ARTIKEL 95 VERHÄLTNIS ZUR RICHTLINIE 2002/58/EG

XI.95.1 Allgemeine Informationen

Thema	Verweis
DSGVO Artikel	Artikel 95 – Verhältnis zur Richtlinie 2002/58/EG (Kapitel XI – Schlussbestimmungen)
DSGVO ErwGr	173
Querverweise	Keine
Zugehörige Unterlagen	Keine
BCRP Verweise	Keine

X.95.2 Zusammenfassung

Die DSGVO gilt für alle Angelegenheiten, die den Schutz der Grundrechte und Grundfreiheiten im Zusammenhang mit der Verarbeitung personenbezogener Daten betreffen, soweit sie nicht besonderen in der ePrivacy-Richtlinie (ePD) festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen. Die ePD umfasst besondere Regelungen für die Verarbeitung personenbezogener Daten im Telekommunikationssektor und im Bereich der elektronischen Kommunikation.

X.95.3 Binding Interpretations

VERHÄLTNIS ZWISCHEN DER EPD UND DER DSGVO:

- Falls die Verarbeitung personenbezogener Daten sowohl der DSGVO als auch der ePD unterliegt, haben die Bestimmungen der nationalen Gesetze zur Umsetzung der ePD Vorrang.
- In der ePD sind Regelungen für die Verarbeitung personenbezogener Daten im Telekommunikationssektor und im Bereich der elektronischen Kommunikation sowie besondere Bestimmungen, zum Beispiel für die Meldung von Vorfällen, Direktwerbung und die Verarbeitung von Standort- und Verkehrsdaten, enthalten.
- Die DSGVO legt einem konzernunternehmen im Zusammenhang mit der ePD keine zusätzlichen Pflichten auf.

ÜBERPRÜFUNG DER EPD:

- Die ePD wird derzeit mit dem Ziel, sie mit der DSGVO zu vereinheitlichen, einer Überprüfung unterzogen.

X.95.4 Fragebogen zur Compliance

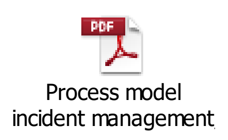
- Verarbeitet Ihr Unternehmen Daten, die bei der Telekommunikation und/oder der elektronischen Kommunikation anfallen? [Ja]/[Nein]
- Falls die Antwort auf die vorherige Frage „ja“ lautete: Verfügt Ihr Unternehmen über ein Verfahren zur Meldung von Vorfällen, die unter den Geltungsbereich der ePD fallen? [Ja]/[Nein]

X.95.5 Sanktionen

Keine

X.95.6 Best Practices und Vorlagen

- Vorlage für die Meldung von Vorfällen auf der Grundlage der ePD und des Prozessmodells Incident Management:



3. ANLAGEN

BEGRIFFSBESTIMMUNGEN

Begriff	Definition
„Ablagesystem“	Bezeichnet jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.
„Aufsichtsbehörde“	Bezeichnet eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle.
„Auftragsverarbeiter“	Bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
„betroffene Aufsichtsbehörde“	Bezeichnet eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil: a) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist, b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.
„biometrische Daten“	Dies sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.
CAPE	Siehe: https://mywiki.telekom.de/pages/viewpage.action?pageId=10485770
„Dienst der Informationsgesellschaft“	Bezeichnet eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates1.

„Direktmarketing“	Bezeichnet Werbung durch Nutzung von E-Mail, Anschrift und Telefonnummer anzustreben
„Dritter“	Bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.
„Einschränkung der Verarbeitung“	Bezeichnet die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.
„Einwilligung“	Die Einwilligung der betroffenen Person bezeichnet jede freiwillig für den bestimmten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
„elektronische Kommunikationsdaten“ als Teil der „elektronischen Kommunikationsdienste“	Bezeichnet gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdiensten in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über solche Inhalte ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen.
„Empfänger“	Bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines besonderen Anfrage nach Unionsrecht oder dem Recht eines Mitgliedstaates möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.
„genetische Daten“	Bezeichnet personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

„Gesundheitsdaten“	Bezeichnet personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.
„grenzüberschreitende Verarbeitung“	Bezeichnet entweder: a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.
„Hauptniederlassung“	Bezeichnet a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung; b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt.
„internationale Organisation“	Bezeichnet eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

„Konzern Deutsche Telekom“	Bezeichnet die Deutsche Telekom AG und alle Unternehmen, an denen die Deutsche Telekom AG mittelbar oder unmittelbar zu mehr als 50 % beteiligt ist oder die vollkonsolidiert sind. Siehe auch Teil 7 der BCRP „Definitionen und Begriffe“.
„maßgeblicher und begründeter Einspruch“	Bezeichnet einen Einspruch gegen einen Beschlussentwurf im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder ob beabsichtigte Maßnahmen in Bezug auf den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung stehen, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen.
„personenbezogene Daten“	Bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
„Profiling“	Bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, diese personenbezogenen Daten zur Bewertung bestimmter Aspekte, die sich auf eine natürliche Person beziehen,zu verwenden, insbesondere um Aspekte wie Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder prognostizieren.
„Pseudonymisierung“	Bezeichnet die Verarbeitung personenbezogener Daten in einer Weise, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und durch technische und organisatorische Maßnahmen gewährleistet wird, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden.
„Unternehmen“	Wird in der DSGVO nicht definiert. Der Begriff wird in der DSGVO in zahlreichen Kontexten verwendet. Am häufigsten bezeichnet er eine juristische Person, die in einer Unternehmensgruppe Wirtschaftstätigkeiten ausübt.

	Im vorliegenden Dokument steht der Begriff „Unternehmen“ beispielsweise für eine Landesgesellschaft (NATCO, LBU) oder eine vollständig konsolidierte Tochtergesellschaft des Konzerns Deutsche Telekom.
„Unternehmensgruppe“	Artikel 4 (19) – Bezeichnet eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.
„Verantwortlicher“	Bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch Unionsrecht oder das Recht eines Mitgliedstaates vorgegeben, so kann der Verantwortliche bzw. können die spezifischen Kriterien für seine Benennung nach Unionsrecht oder dem Recht des Mitgliedstaates festgelegt sein.
„Verarbeitung“	Bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie die Erhebung, Erfassung, die Organisation, Sortierung, Speicherung, Anpassung oder Veränderung, Auslesung, Abfrage, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleichung oder Verknüpfung, Einschränkung, Löschung oder Vernichtung.
„verbindliche interne Datenschutzvorschriften“	Bezeichnet Maßnahmen zum Schutz personenbezogener Daten, die ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter beachtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern.
„Verletzung des Schutzes personenbezogener Daten“	Bezeichnet eine Verletzung der Sicherheit, die – unbeabsichtigt oder unrechtmäßig – zuVernichtung, Verlust, Veränderung oder unbefugter Offenlegung von übermittelten, gespeicherten oder sonstwie verarbeiteten personenbezogenen Daten führt bzw. unbefugten Zugang zu solchen Daten ermöglicht.
„Vertreter“	Bezeichnet eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt.
„Wirtschaftsunternehmen“	Bezeichnet eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich

	Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

ABKÜRZUNGEN

Begriff	Abkürzung
Art.	Artikel
BCRP	Konzernrichtlinie Datenschutz – Binding Corporate Rules Privacy
BDSG	Bundesdatenschutzgesetz
CAPE	Die Software CAPE ist Teil der Zertifizierung des Privacy-Compliance-Management-Systems des Konzerns Deutsche Telekom nach dem Wirtschaftsprüfungsstandard 980.
CDPA	Vertrag über die Auftragsdatenverarbeitung („Commissioned Data Processing Agreement“)
CSV	Computersystemvalidierung
DSFA	Datenschutz-Folgenabschätzungen
DSB	Datenschutzbeauftragter
DT	Deutsche Telekom
EWR	Europäischer Wirtschaftsraum
z.B.	Zum Beispiel
ePD	ePrivacy-Richtlinie („ePrivacy Directive“)
EU	Europäische Union
DSGVO	Datenschutz-Grundverordnung
GPR	Group Privacy
KEK	Konzernweite Einwilligungsklausel
LBU	Local Business Unit
NatCo	Landesgesellschaft
PSA	Privacy und Security Assessment
ErwGr	Erwägungsgrund
SDM	Security Demand Management
SDSK	Standardisiertes Datenschutz- und Sicherheitskonzept
TOM	Technische und organisatorische Maßnahmen

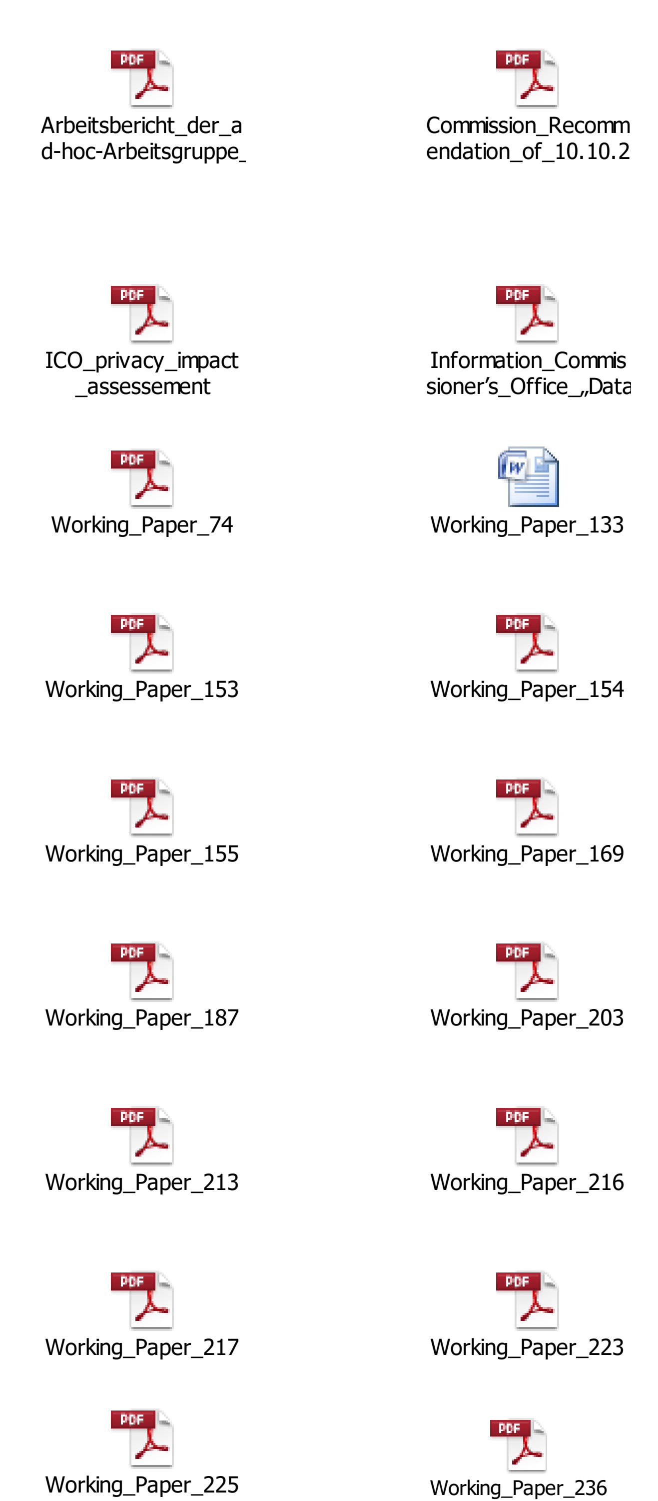
4. ANHANG



GDPR - Text.docx



BCRP.pdf


Arbeitsbericht_der_a
d-hoc-Arbeitsgruppe_
Commission_Recomm
endation_of_10.10.2
ICO_privacy_impact
_assessement
Information_Commis
sioner's_Office_„Data
Working_Paper_74
Working_Paper_133
Working_Paper_153
Working_Paper_154
Working_Paper_155
Working_Paper_169
Working_Paper_187
Working_Paper_203
Working_Paper_213
Working_Paper_216
Working_Paper_217
Working_Paper_223
Working_Paper_225
Working_Paper_236